JP2005015085 / 2006-019143

1/3

Date: Feb 23, 2006

Recipient: IB

Address: Bureau international de l'OMPI 34, chemin des Colombettes Geneve 20 1211 CH

明 細 書

イベント順序証明方法

技術分野

[0001] 本発明は、デジタル・データの生成を伴うイベントの生起順序を証明するイベント順序証明技術に関する。

背景技術

[0002] イベント順序証明技術は、デジタル・データの生成を伴う複数のイベント間の生起順序を証明するとともに、そのようなイベントに伴って生成されたデジタル・データが何であったかを証明する技術である。

[0003] 近年、インターネット上での電子商取引の活発化や、デジタル文書管理の利用拡大に伴い、「誰が、いつ、どんなデータを生成し、交信したか」を第三者が証明する電子公証の仕組みが必要とされている。電子公証は、送受信者の特定、到達確認、送受信等の前後関係の証明、改ざんの検知、電子文書保管等の機能を具備するものであるが、イベント順序証明技術は、このうち、前後関係の証明及び改ざんの検知の機能を実現するものである。

[0004] 図1は、このようなイベント順序証明技術を用いたイベント順序証明システムを説明する図である。同図に示すイベント順序証明システム900は、利用者(要求者、検証者)30がイベント順序証明の対象データをイベント順序証明装置10に送信すると、イベント順序証明装置10が利用者30から要求された対象データに対して受付の順番を示すデータを付したイベント順序受理証明書を生成し、該イベント順序受理証明書を利用者に返信するようになっている。そして、イベント順序証明装置10で発行されたイベント順序受理証明書は、PKI(Public Key Infrastructure;公開鍵基盤)のもとでデジタル署名を主要な偽造防止/証明手段として採用する場合には、一般に、利用者30から送られた対象データに受付の順番を付した署名対象データに対するデジタ

ル署名を含んだイベント順序受理証明書となっている。

[0005] このイベント順序受理証明書の真正性の主要な根拠としてデジタル署名を用いるイベント順序証明システムに関しては、イベント順序証明装置 10の不正、イベント順序受理証明書の有効期間、およびシステム運用の面などにおいて問題点が指摘されている。そのため、イベント順序受理証明書の真正性の主要な根拠としてデジタル署名を用いないイベント順序証明の方法も提案されている。例えば、線形リンキング(Linear Linking Protocol)による方法(例えば、非特許文献1及び非特許文献2参照。)は、イベント順序証明装置10が仮に信頼できないとしてもシステム全体として高い安全性を確保することが可能となっている方法である。図2は、PKIに依存しない線形リンキングによるイベント順序証明システムを説明する図である。同図に示すイベント順序証明システム910は、複数の利用者30のイベント順序証明対象データ(ハッシュ値)を相互に関連付けるリンク情報L_nを生成し、リンク情報L_nを含むイベント順序受理証明書を返信するようになっており、各イベント順序受理証明書が、それまでに生成されたすべてのイベント順序受理証明書に依存するようになっている。そして、このリンク情報の一部(L_M, L_N)が定期的にマスメディア等(例えば新聞)に公表されるので、これにより、イベント順序証明装置10の不正を防止し、結果としてシステム全体の信頼を高めることができるようになっている。

[0006] この線形リンキングの方式については、イベント順序証明装置10の不正を検出するために利用者30相互の協力が必要であるという問題点、及び、利用者30が取得したイベント順序受理証明書を検証、即ち、該イベント順序受理証明書と公表された情報が所定の方式で関係づけられることを検証するには利用者30はイベント順序証明装置10から大量のデータを取得する必要があるという問題点が指摘されている。

[0007] これらの問題の一部を解決するための方法も提案されている。例えば、非特許文献3及び非特許文献4においては、一定期間にイベント順序証明装置で処理されたイベント順序証明要求をまとめ公表するデータを計算するために、非特許文献1及び非特許文献2で使われている線形のリストの代わりに、木構造を用いることにより、利用者30がイベント順序受理証明書の検証を行うために必要なデータの量を、該一定期間に受付けられるイベント順序証明要求の数に比例する量から、その対数(底2)

に比例する量に著しく削減する方法を提案している。

非特許文献1:S. Haber and W. Stornetta, How to Time-Stamp a Digital Document, Journal of Cryptology, Vol. 3, No. 2, pp. 99__111, 1991

非特許文献2:J.-J. Quisquater, H. Massias, J.S. Avila, B. Preneel, B. Van Rompay: Specification and implementation of a timestamping system, Technical Report of Uni versite Catholique de Louvain, 1999,URL: http://www.dice.ucl.ac.be/crypto/TIME SEC/TR4.tgzl

非特許文献3:A. Buldas、H. Lipmaa and B. Schoenmakers, Optim ally efficient accountable time-stamping, in Proceedings of Public Key Cryptography 2000 (PKC2000), eds. Y. Zheng and H. Imai, pp.293__305, Springer-Verlag, Janu ary 2000

非特許文献4:A. Buldas、H. Lipmaa and B. Schoenmakers, Optim ally efficient accountable time-stamping, in Proceedings of Public Key Cryptography 2000 (PKC2000), eds. Y. Zheng and H. Imai, pp.293-305, Springer-Verlag, Janua ry 2000

発明の開示

[0008] しかしながら、非特許文献3及び非特許文献4に記載の木構造を用いる方式については、次のような問題点がある。

[0009] ある一定期間に異なる2つの利用者が各々イベント順序証明要求をイベント順序証明装置に送付し、それら要求が受理されたときにおいて、第1の利用者のある順序証明要求の受付けが第2の利用者のある順序証明要求の受付けより前になされたことの証明が、当該の期間が終了してイベント順序証明要求をまとめた公表データが公開されるまではできないという問題がある。即ち、当該の2つの順序証明要求と公表データが所定の方式で関係付けられることの検証が、公表データが公開されるまでできないという問題がある。このため、イベント順序証明システムに対する利用者の利便性が劣るとともに、イベント順序証明装置に障害が発生した時には、イベント順序受理証明書の検証ができないという欠点がある。

[0010] 本発明は、上記の問題を解決するためになされたものであり、木構造を用いてイベ

ント順序を証明するイベント順序証明システムにおいて、イベント順序証明要求をまとめた公表データを用いなくても、イベント順序証明機関から発行されたイベント順序受理証明書の検証を行うことができるイベント順序証明方法及びイベント順序証明監査方法、イベント順序証明システムにおける証明装置及び監査装置、並びにイベント順序証明プログラム、イベント順序証明監査プログラム、イベント順序証明検証プログラム及びイベント時刻検証プログラムを提供することを目的とする。

[0011] 本発明の第1の側面は、所定のデジタル情報を生成するイベントの時系列において、あるイベントを生成した相対的な時刻、即ち時間的順序、を証明する証明要求を行う利用者装置と、前記利用者装置からの前記証明要求に対する証明書を作成する証明装置と、前記証明書の真偽を監査する監査装置とが通信ネットワークを介して相互に接続されたイベント順序証明システムにおけるイベント順序証明方法であって、前記証明装置が前記利用者装置からの証明要求を受信する順序証明要求受信ステップと、前記証明装置が前記証明要求に含まれるデジタル情報から予め定めた手順に従って順次割当データを作成する順次割当データ計算ステップと、前記証明装置が、一連の順次割当データを時刻順に有向木のリーフに左から順次割り当てることによって一定時間間隔ごとに1つの集約木が生成される順次集約木において、同一の親を有する複数の子に割り当てられたそれぞれの割当値を連接した連接値に所定の衝突困難一方向関数を適用した結果値を前記親の割当値とする計算方法により、計算可能なノードの割当値を計算するとともに、前記一定時間間隔終了後に前記順次集約木のルートに割り当てるルート値を計算する順序証明要求集約ステップと、前記証明装置が、前記順次割当データ、並びに前記順次割当データが割り当てられた順次集約木及び該順次集約木のリーフを特定する第1の順次集約木特定情報を含む証明書を作成する証明書作成ステップと、前記証明装置が前記証明書を前記利用者装置に送信する証明書送信ステップと、前記証明要求が割り当てられた前記順次集約木のリーフを登録点と定義し、該登録点から前記順次集約木のルート値を計算するのに必要なノードに関する情報を前記証明書の補完情報と定義し、該補完情報のうち、前記証明要求を前記順次集約木に割り当てた時点において取得可能な補完情報を即時補完情報と定義すると、前記証明装置が、前記証明要求を

前記順次集約木に割り当てた以後に、第1の監査要求を前記順次集約木に割り当て、前記証明書と同一の作成方法により、第1の監査用証明書を作成するとともに、前記監査要求を前記順次集約木に割り当てた時点における第1の監査用の即時補完情報を前記順次集約木から取得し、前記第1の監査用証明書に含める監査用証明書作成ステップと、前記証明装置が前記第1の監査用証明書を前記監査装置に送信する監査用証明書送信ステップと、前記証明装置が、前記第1の監査要求を前記順次集約木に割り当てた以後に、前記利用者装置からの前記証明書の補完情報の要求を受信する補完情報要求受信ステップと、前記証明装置が、前記補完情報の要求が割り当てられた前記順次集約木及び前記順次集約木のリーフを特定する第2の順次集約木特定情報、及び前記補完情報の要求を割り当てた時点において取得可能な補完情報を前記順次集約木から取得し、遅延補完情報とする遅延補完情報作成ステップと、前記証明装置が前記証明書の前記遅延補完情報を前記利用者装置に送信する遅延補完情報送信ステップと、を有することを特徴とする。

[0012] 本発明の第2の側面は、所定のデジタル情報を生成するイベントの時系列において、あるイベントを生成した相対的な時刻、即ち時間的順序、を証明する証明要求を行う少なくとも1つの利用者装置と、利用者装置からの証明要求に対する証明書を作成する証明装置と、前記証明書の真偽を監査する監査装置とが通信ネットワークを介して相互に接続されたイベント順序証明システムにおけるイベント順序証明監査方法であって、前記証明装置が前記利用者装置から第1の証明要求を受信する順序証明要求受信ステップと、前記証明装置が前記第1の証明要求に含まれるデジタル情報から予め定めた手順に従って順次割当データを作成する順次割当データ計算ステップと、前記証明装置が、一連の順次割当データを時刻順に有向木のリーフに左から順次割り当てることによって一定時間間隔ごとに1つの集約木が生成される順次集約木において、同一の親を有する複数の子に割り当てられたそれぞれの割当値を連接した連接値に所定の衝突困難一方向関数を適用した結果値を前記親の割当値とする計算方法により、計算可能なノードの割当値を計算するとともに、前記一定時間間隔終了後に前記順次集約木のルートに割り当てるルート値を計算する順序証明要求集約ステップと、前記証明装置が、前記順次割当データ、並びに前記順次

割当データが割り当てられた順次集約木及び該順次集約木のリーフを特定する第1の順次集約木特定情報を含む第1の証明書を作成する証明書作成ステップと、前記証明装置が前記第1の証明書を前記利用者装置に送信する証明書送信ステップと、前記第1の証明要求が割り当てられた前記順次集約木のリーフを登録点として定義し、該登録点から前記順次集約木のルート値を計算するのに必要なノードに関する情報を前記第1の証明書の補完情報と定義し、該補完情報のうち、前記第1の証明要求を前記順次集約木に割り当てた時点において取得可能な補完情報を即時補完情報と定義すると、前記証明装置が、複数の監査要求を前記順次集約木に割り当て、前記第1の証明書と同一の作成方法により、複数の監査用証明書を作成するとともに、各監査要求を前記順次集約木に割り当てた時点における監査用の即時補完情報を前記順次集約木から取得し、各監査用証明書に含める監査用証明書作成ステップと、前記証明装置が前記複数の監査用証明書を前記監査装置に送信する監査用証明書送信ステップと、前記証明装置が、前記第1の証明書送信後に、前記利用者装置からの前記第1の証明書の補完情報の要求を受信する補完情報要求受信ステップと、前記証明装置が、前記補完情報の要求が割り当てられた前記順次集約木及び前記順次集約木のリーフを特定する第2の順次集約木特定情報、及び前記補完情報の要求を割り当てた時点において取得可能な補完情報を前記順次集約木から取得し、遅延補完情報とする遅延補完情報作成ステップと、前記証明装置が前記第1の証明書の前記遅延補完情報を前記利用者装置に送信する遅延補完情報送信ステップと、前記監査装置が、前記証明装置から前記複数の監査用証明書を受信する監査用証明書受信ステップと、前記監査装置が、前記利用者装置から前記第1の証明書及び前記第1の証明書の前記遅延補完情報を含む前記第1の証明書に対する監査要求を受信する監査要求受信ステップと、前記監査装置が、前記複数の監査用証明書の中から、前記第1の証明書に対する監査要求の第1及び第2の順次集約木特定情報に基づいて、前記第1の証明書より生成された時間的順序が後、かつ前記遅延補完情報より生成された時間的順序が前である監査用証明書を選択する第1の監査用証明書選択ステップと、前記監査装置が、前記順次集約木の特定のノードに対して、前記第1の監査用証明書選択ステップで選択された監査用証明書に

含まれる該ノードの割当値と、前記第1の証明書に対する監査要求から計算された該ノードの割当値が一致するか否かの検証に基づいて、前記第1の証明書の正当性を監査し、前記第1の証明書の証明要求の受付時刻と前記第1の監査用証明書選択ステップで選択された監査用証明書の監査要求の受付時刻との前後関係を証明する第1の証明書監査ステップと、前記監査装置が前記第1の証明書の監査結果を前記利用者装置に送信する監査結果送信ステップと、を有することを特徴とする。

[0013] 本発明の第3の側面は、所定のデジタル情報を生成するイベントの時系列において、あるイベントを生成した相対的な時刻、即ち時間的順序、を証明する証明要求を行い、証明書の作成を促す利用者装置と、該証明書の真偽を監査する監査装置とに通信ネットワークを介して相互に接続され、前記証明書を作成するイベント順序証明装置であって、前記利用者装置から証明要求を受信する順序証明要求受信手段と、前記証明要求に含まれるデジタル情報から予め定めた手順に従って順次割当データを作成する順次割当データ計算手段と、一連の順次割当データを時刻順に有向木のリーフに左から順次割り当てることによって一定時間間隔ごとに1つの集約木が生成される順次集約木において、同一の親を有する複数の子に割り当てられたそれぞれの割当値を連接した連接値に所定の衝突困難一方向関数を適用した結果値を前記親の割当値とする計算方法により、計算可能なノードの割当値を計算するとともに、前記一定時間間隔終了後に前記順次集約木のルートに割り当てるルート値を計算する順序証明要求集約手段と、前記順次割当データ、並びに前記順次割当データが割り当てられた順次集約木及び該順次集約木のリーフを特定する第1の順次集約木特定情報を含む証明書を作成する証明書作成手段と、前記証明書を前記利用者装置に送信する証明書送信手段と、前記証明要求が割り当てられた前記順次集約木のリーフを登録点と定義し、該登録点から前記順次集約木のルート値を計算するのに必要なノードに関する情報を前記証明書の補完情報と定義し、該補完情報のうち、前記証明要求を前記順次集約木に割り当てた時点において取得可能な補完情報を即時補完情報と定義すると、前記証明要求を前記順次集約木に割り当てた以後に、第1の監査要求を前記順次集約木に割り当て、前記証明書と同一の作成方法により、第1の監査用証明書を作成するとともに、前記第1の監査要求を前記順

次集約木に割り当てた時点における第1の監査用の即時補完情報を前記順次集約木から取得し、該第1の監査用証明書に含める監査用証明書作成手段と、前記第1の監査用証明書を前記監査装置に送信する監査用証明書送信手段と、前記第1の監査要求を前記順次集約木に割り当てた以後に、前記利用者装置からの前記証明書の補完情報の要求を受信する補完情報要求受信手段と、前記補完情報の要求が割り当てられた前記順次集約木及び前記順次集約木のリーフを特定する第2の順次集約木特定情報、及び前記補完情報の要求を割り当てた時点において取得可能な補完情報を前記順次集約木から取得し、遅延補完情報とする遅延補完情報作成手段と、前記証明書の前記遅延補完情報を前記利用者装置に送信する遅延補完情報送信手段と、を有することを特徴とする。

[0014] 本発明の第4の側面は、所定のデジタル情報を生成するイベントの時系列において、あるイベントを生成した相対的な時刻、即ち時間的順序、を証明する証明要求を行う少なくとも1つの利用者装置と、利用者装置からの証明要求に対する証明書を作成する証明装置とに通信ネットワークを介して接続され、前記証明書の真偽を監査するイベント順序証明監査装置であって、前記証明装置は、前記利用者装置からの第1の証明要求を受信する順序証明要求受信手段と、前記第1の証明要求に含まれるデジタル情報から予め定めた手順に従って順次割当データを作成する順次割当データ計算手段と、一連の順次割当データを時刻順に有向木のリーフに左から順次割り当てることによって一定時間間隔ごとに1つの集約木が生成される順次集約木において、同一の親を有する複数の子に割り当てられたそれぞれの割当値を連接した連接値に所定の衝突困難一方向関数を適用した結果値を前記親の割当値とする計算方法により、計算可能なノードの割当値を計算するとともに、前記一定時間間隔終了後に前記順次集約木のルートに割り当てるルート値を計算する順序証明要求集約手段と、前記順次割当データ、並びに前記順次割当データが割り当てられた順次集約木及び該順次集約木のリーフを特定する第1の順次集約木特定情報を含む第1の証明書を作成する証明書作成手段と、前記第1の証明書を前記利用者装置に送信する証明書送信手段と、前記第1の証明要求が割り当てられた前記順次集約木のリーフを登録点と定義し、該登録点から前記順次集約木のルート値を計算するのに

必要なノードに関する情報を前記第1の証明書の補完情報と定義し、該補完情報のうち、前記第1の証明要求を前記順次集約木に割り当てた時点において取得可能な補完情報を即時補完情報と定義すると、複数の監査要求を前記順次集約木に割り当て、前記第1の証明書と同一の作成方法により、複数の監査用証明書を作成するとともに、前記複数の監査要求を前記順次集約木に割り当てた時点における監査用の前記即時補完情報を前記順次集約木から取得し、各監査用証明書に含める監査用証明書作成手段と、前記複数の監査用証明書を前記監査装置に送信する監査用証明書送信手段と、前記第1の証明書送信後に、前記利用者装置からの前記第1の証明書の補完情報の要求を受信する補完情報要求受信手段と、前記補完情報の要求が割り当てられた前記順次集約木及び前記順次集約木のリーフを特定する第2の順次集約木特定情報、及び前記補完情報の要求を割り当てた時点において取得可能な補完情報を前記順次集約木から取得し、遅延補完情報とする遅延補完情報作成手段と、前記第1の証明書の前記遅延補完情報を前記利用者装置に送信する遅延補完情報送信手段と、を備え、前記証明装置から前記複数の監査用証明書を受信する監査用証明書受信手段と、前記利用者装置から前記第1の証明書及び前記遅延補完情報を含む前記第1の証明書に対する監査要求を受信する監査要求受信手段と、前記複数の監査用証明書の中から、前記第1の証明書に対する監査要求の第1及び第2の順次集約木特定情報に基づいて、前記第1の証明書より生成された時間的順序が後、かつ前記遅延補完情報より生成された時間的順序が前である監査用証明書を選択する第1の監査用証明書選択手段と、前記順次集約木の特定のノードに対して、前記第1の監査用証明書選択手段で選択された監査用証明書に含まれる該ノードの割当値と、前記第1の証明書に対する監査要求から計算された該ノードの割当値が一致するか否かの検証に基づいて、前記第1の証明書の正当性を監査し、前記第1の証明書の証明要求の受付時刻と前記第1の監査用証明書選択手段によって選択された監査用証明書の監査要求の受付時刻との前後関係を証明する第1の証明書監査手段と、前記第1の証明書の監査結果を前記利用者装置に送信する監査結果送信手段と、を備えることを特徴とする。

[0015] 本発明の第5の側面は、上記したイベント順序証明方法の各ステップを前記証明装

置に実行させるイベント順序証明プログラムを提供することにある。

[0016] 本発明の第6の側面は、上記したイベント順序証明監査方法の各ステップを前記監査装置に実行させるイベント順序証明監査プログラムを提供することにある。

[0017] 本発明の第7の側面は、所定のデジタル情報を生成するイベントの時系列において、あるイベントを生成した相対的な時刻、即ち時間的順序、を証明する証明要求を行う少なくとも1つの利用者装置と、利用者装置からの証明要求に対する証明書を作成する証明装置と、前記証明書の真偽を監査する監査装置とが通信ネットワークを介して相互に接続されたイベント順序証明検証システムにおける前記利用者装置のためのイベント順序証明検証プログラムであって、前記証明装置は、前記利用者装置からの第1の証明要求を受信する順序証明要求受信手段と、前記第1の証明要求に含まれるデジタル情報から予め定めた手順に従って順次割当データを作成する順次割当データ計算手段と、一連の順次割当データを時刻順に有向木のリーフに左から順次割り当てることによって一定時間間隔ごとに1つの集約木が生成される順次集約木において、同一の親を有する複数の子に割り当てられたそれぞれの割当値を連接した連接値に所定の衝突困難一方向関数を適用した結果値を前記親の割当値とする計算方法により、計算可能なノードの割当値を計算するとともに、前記一定時間間隔終了後に前記順次集約木のルートに割り当てるルート値を計算する順序証明要求集約手段と、前記順次割当データ、並びに前記順次割当データが割り当てられた順次集約木及び該順次集約木のリーフを特定する第1の順次集約木特定情報を含む第1の証明書を作成する証明書作成手段と、前記第1の証明書を前記利用者装置に送信する証明書送信手段と、前記第1の証明要求が割り当てられた前記順次集約木のリーフを登録点と定義し、該登録点から前記順次集約木のルート値を計算するのに必要なノードに関する情報を前記第1の証明書の補完情報と定義し、該補完情報のうち、前記第1の証明要求を前記順次集約木に割り当てた時点において取得可能な補完情報を即時補完情報と定義すると、複数の監査要求を前記順次集約木に割り当て、前記第1の証明書と同一の作成方法により、複数の監査用証明書を作成するとともに、前記複数の監査要求を前記順次集約木に割り当てた時点におけるそれぞれの監査用の即時補完情報を前記順次集約木から取得し、前記複数の監

査用証明書に含める監査用証明書作成手段と、前記複数の監査用証明書を前記監査装置に送信する監査用証明書送信手段と、前記第1の証明書送信後に、前記利用者装置からの前記第1の証明書の補完情報の要求を受信する補完情報要求受信手段と、前記補完情報の要求が割り当てられた前記順次集約木及び前記順次集約木のリーフを特定する第2の順次集約木特定情報、及び前記補完情報の要求を割り当てた時点において取得可能な補完情報を前記順次集約木から取得し、遅延補完情報とする遅延補完情報作成手段と、前記第1の証明書の前記遅延補完情報を前記利用者装置に送信する遅延補完情報送信手段と、を有し、前記監査装置は、前記証明装置から、前記複数の監査用証明書を受信する監査用証明書受信手段と、前記利用者装置から、前記第1の証明書及び前記遅延補完情報を含む前記第1の証明書に対する監査要求を受信する監査要求受信手段と、前記複数の監査用証明書の中から、前記第1の証明書に対する監査要求の第1及び第2の順次集約木特定情報に基づいて、前記第1の証明書より生成された時間的順序が後、かつ前記遅延補完情報より生成された時間的順序が前である監査用証明書を選択する第1の監査用証明書選択手段と、前記順次集約木の特定のノードに対して、前記第1の監査用証明書選択手段によって選択された監査用証明書に含まれる該ノードの割当値と、前記第1の証明書に対する監査要求から計算された該ノードの割当値が一致するか否かの検証に基づいて、前記第1の証明書の正当性を監査し、前記第1の証明書の証明要求の受付時刻と前記第1の監査用証明書選択手段によって選択された監査用証明書の監査要求の受付時刻の前後関係を証明する第1の証明書監査手段と、前記第1の証明書の監査結果を前記利用者装置に送信する監査結果送信手段と、を有し、前記第1の証明要求を前記証明装置に送信する順序証明要求送信ステップと、前記証明装置から、前記第1の証明書を受信する証明書受信ステップと、前記第1の証明書の前記補完情報の要求を前記証明装置に送信する補完情報要求送信ステップと、前記証明装置から、前記第1の証明書の前記補完情報を受信する補完情報受信ステップと、前記監査要求を前記監査装置に送信する監査要求送信ステップと、前記第1の証明書の監査結果を受信する監査結果受信ステップと、を前記利用者装置に実行させることを特徴とする。

[0018] 本発明の第8の側面は、所定のデジタル情報を生成するイベントの時系列において、あるイベントを生成した相対的な時刻、即ち時間的順序、を証明する証明要求を行う第1及び第2の利用者装置と、各利用者装置からの複数の証明要求に対して複数の証明書を作成するイベント順序証明装置とに通信ネットワークを介して相互に接続されたコンピュータに証明書の正当性を検証させるイベント順序証明検証プログラムであって、前記イベント順序証明装置は、前記第1及び第2の利用者装置から複数の証明要求を受信する順序証明要求受信手段と、各証明要求に含まれるデジタル情報から予め定めた手順に従って順次割当データを作成する順次割当データ計算手段と、一連の順次割当データを時刻順に有向木のリーフに左から順次割り当て、一定時間間隔ごとに1つの集約木が生成される順次集約木において、同一の親を有する複数の子に割り当てられたそれぞれの割当値を連接した連接値に所定の衝突困難一方向関数を適用した結果値を前記親の割当値とする計算方法により、計算可能なノードの割当値を計算するとともに、前記一定時間間隔終了後に前記順次集約木のルートに割り当てるルート値を計算する順序証明要求集約手段と、前記順序証明要求集約手段で生成される順次集約木に関する情報を記憶する順次集約木記憶手段と、各証明要求から作成された順次割当データが割り当てられた前記順次集約木のリーフを登録点と定義し、該登録点から前記順次集約木のルート値を計算するのに必要なノードに関する情報を前記登録点の補完情報と定義し、該補完情報のうち、前記順次割当データを前記順次集約木に割り当てた時点において取得可能な補完情報を即時補完情報、前記順次割当データを前記順次集約木に割り当てた時点以後において取得可能な補完情報を遅延補完情報と定義し、リーフa1より右に位置するリーフa2の割当処理が終了した時点で定まる前記リーフa1の遅延補完情報を、前記リーフa1の前記リーフa2における遅延補完情報といい、さらに、最新の前記要求から作成された順次割当データが割り当てられた前記順次集約木のリーフを新登録点とすると、利用者装置ごとに前記複数の証明要求の登録点に関する情報を記憶する登録点記憶手段と、各記憶手段によって記憶された情報から、該新登録点の順次割当データと、該順次割当データが割り当てられた前記順次集約木及び該順次集約木のリーフを特定する順次集約木特定情報と、前記新登録点の即時補完情報

と、各利用者装置の過去のすべての登録点の新登録点における遅延補完情報と、を併せることによって前記新登録点に対する証明書を作成する証明書作成手段と、前記作成された複数の証明書を前記利用者装置に送信する証明書送信手段と、を有し、各利用者装置は、複数の証明要求を前記イベント順序証明装置に送信する証明要求送信手段と、前記イベント順序証明装置から前記複数の証明要求に対する前記複数の証明書を受信する証明書受信手段と、前記受信した複数の証明書を記憶する証明書記憶手段と、前記受信し記憶した複数の証明書のうち、検証対象の証明書を検証するコンピュータに送信する検証要求送信手段と、前記コンピュータから前記検証対象の証明書に対する検証結果を受信する検証結果受信手段と、を有し、前記第1及び第2の利用者装置から検証対象の証明書を1つずつ受信するか、或いは前記第1の前記利用者装置から検証対象の証明書を2つ受信する証明書受信ステップと、前記受信した2つの証明書の順次集約木特定情報に基づいて、前記2つの証明書のうち発行された順序が時間的に前であると判断された証明書を第1の証明書、後であると判断された証明書を第2の証明書とすると、前記第1の証明書を送信した利用者装置に対して前記第2の証明書の順次集約木特定情報を送信する順次集約木特定情報送信ステップと、前記第1の証明書を送信した利用者装置から、前記第1の証明書の前記第2の証明書の発行以降の登録点における遅延補完情報を受信する遅延補完情報受信ステップと、前記順次集約木の特定のノードに対して、前記第2の証明書に含まれるノードの割当値と、前記第1の証明書および前記遅延補完情報から計算されたノードの割当値が一致するか否かの検証に基づいて、各証明書の正当性及び前記第1の証明書の登録点が前記第2の証明書の登録点より時間的に前であることを証明する検証ステップと、検証結果を前記第1及び第2の利用者装置、或いは前記第1又は第2の利用者装置に送信する検証結果送信ステップと、を前記コンピュータに実行させることを特徴とする。

[0019] 本発明の第9の側面は、所定のデジタル情報を生成するイベントの時系列において、あるイベントを生成した相対的な時刻、即ち時間的順序、を証明する証明要求を行う第1及び第2の利用者装置と、各利用者装置からの複数の証明要求に応えて複数の証明書を作成するイベント順序証明装置とに通信ネットワークを介して相互に接

続されたコンピュータに証明書の正当性を検証させるイベント順序証明検証プログラムであって、前記イベント順序証明装置は、前記第1及び第2の利用者装置から複数の証明要求を受信する順序証明要求受信手段と、各証明要求に含まれるデジタル情報から予め定めた手順に従って順次割当データを作成する順次割当データ計算手段と、一連の順次割当データを時刻順に有向木のリーフに左から順次割り当て、一定時間間隔ごとに1つの集約木が生成される順次集約木において、同一の親を有する複数の子に割り当てられたそれぞれの割当値を連接した連接値に所定の衝突困難一方向関数を適用した結果値を前記親の割当値とする計算方法により、計算可能なノードの割当値を計算するとともに、前記一定時間間隔終了後に前記順次集約木のルートに割り当てるルート値を計算する順序証明要求集約手段と、前記順序証明要求集約手段で生成される順次集約木に関する情報を記憶する順次集約木記憶手段と、各証明要求から作成された順次割当データが割り当てられた前記順次集約木のリーフを登録点と定義し、該登録点から前記順次集約木のルート値を計算するのに必要な他のノードに関する情報を前記登録点の補完情報と定義し、該補完情報のうち、前記順次割当データを前記順次集約木に割り当てた時点において取得可能な補完情報を即時補完情報、前記順次割当データを前記順次集約木に割り当てた時点以後において取得可能な補完情報を遅延補完情報と定義し、リーフa1より右に位置するリーフa2の割当処理が終了した時点で定まる前記リーフa1の遅延補完情報を、前記リーフa1の前記リーフa2における遅延補完情報といい、さらに、最新の前記要求から作成された順次割当データが割り当てられた前記順次集約木のリーフを新登録点とすると、利用者装置ごとに前記直前の登録点に関する情報を記憶する登録点記憶手段と、各記憶手段によって記憶された情報から、該新登録点の順次割当データと、該順次割当データが割り当てられた順次集約木及び該順次集約木のリーフを特定する順次集約木特定情報と、新登録点の即時補完情報と、前記利用者装置の前記直前の登録点の前記新登録点における遅延補完情報と、を併せることによって前記新登録点に対する証明書を作成する証明書作成手段と、作成された証明応答を前記利用者装置に送信する証明応答送信手段と、を有し、各利用者装置の各登録点のうち、前記順次集約木の最も右に割り付けられた登録点を暫定終端点と

し、該暫定終端点の割付処理が終了した時点において、所定の登録点の取得可能な補完情報すべてを計算することを、前記所定の登録点の証明書に対するインクリメンタル完全化と定義すると、各利用者装置は、複数の証明要求を前記イベント順序証明装置に送信する証明要求送信手段と、前記イベント順序証明装置から前記複数の証明要求に対する前記複数の証明書を受信する証明書受信手段と、前記受信した複数の証明書を記憶する証明書記憶手段と、前記受信し記憶した複数の証明書のうち、検証対象の証明書に対して前記インクリメンタル完全化の処理を行うインクリメンタル完全化手段と、前記インクリメンタル完全化された証明書を検証する検証要求をコンピュータに送信する検証要求送信手段と、前記コンピュータから前記検証対象の前記証明書に対する検証結果を受信する検証結果受信手段と、を有し、前記第1及び第2の利用者装置から検証対象の証明書を1つずつ受信するか、或いは前記第1の利用者装置から検証対象の証明書を2つ受信する証明書受信ステップと、前記受信した2つの証明書の順次集約木特定情報に基づいて、前記2つの証明書のうち発行された順序が時間的に前であると判断された証明書を第1の証明書、後であると判断された証明書を第2の証明書とすると、前記第1の証明書を送信した利用者装置に、前記第2の証明書の順次集約木特定情報を送信する順次集約木特定情報送信ステップと、前記第1の証明書を送信した利用者装置から、前記第1の証明書の前記第2の証明書の発行以降の登録点における遅延補完情報を受信する遅延補完情報受信ステップと、前記順次集約木の特定のノードに対して、前記第2の証明書に含まれるノードの割当値と、前記第1の証明書および前記遅延補完情報から計算されたノードの割当値が一致するか否かの検証に基づいて、各証明書の正当性及び前記第1の証明書の登録点が前記第2の証明書の登録点より時間的に前であることを証明する検証ステップと、検証結果を前記第1及び第2の利用者装置、或いは前記第1又は第2の利用者装置に送信する検証結果送信ステップと、を前記コンピュータに実行させることを特徴とする。

[0020] 本発明の第10の側面は、上記のイベント順序証明検証プログラムを実行する利用者装置が前記証明要求に付した時刻を検証するコンピュータが読み取り可能なイベント時刻検証プログラムを提供することにある。

図面の簡単な説明

[0021] [図1]図1は、イベント順序証明システムの概念を説明する図である。

[図2]図2は、線形リンキングを用いたイベント順序証明システムの概念を説明する図である。

[図3]図3は、本発明の第1の実施の形態に係るイベント順序証明システムのシステム構成図である。

[図4]図4は、本発明の第1の実施の形態に係るイベント順序証明システムの別のシステム構成図である。

[図5]図5は、本発明に用いられる順次集約木の構成を説明する図である。

[図6]図6は、本発明におけるイベント順序受理証明書の構成を説明する図である。

[図7]図7は、本発明に用いられる順次集約木の認証パスを説明する図である。

[図8]図8は、本発明の第1の実施の形態に係るイベント順序証明システムのイベント順序証明方法を説明するシーケンス図である。

[図9]図9は、本発明の第1の実施の形態に係るイベント順序証明システムのイベント順序証明検証方法を説明するシーケンス図である。

[図10]図10は、本発明の第1の実施の形態に係るイベント順序証明システムのイベント順序証明検証方法を説明するシーケンス図である。

[図11]図11は、本発明の第1の実施の形態に係るイベント順序証明システムにおけるユーザ点と監査点の関係を説明する図である。

[図12]図12は、本発明の第1の実施の形態に係るイベント順序証明システムのイベント順序証明検証結果を説明する図である。

[図13]図13は、本発明の第2の実施の形態に係るイベント順序証明システムのシステム構成図である。

[図14]図14は、本発明の第2の実施の形態に係るイベント順序証明システムにおけるユーザ点と監査点の関係を説明する図である。

[図15]図15は、本発明の第2の実施の形態に係るイベント順序証明システムのイベント順序証明方法を説明するシーケンス図である。

[図16]図16は、本発明の第2の実施の形態に係るイベント順序証明システムのイベ

ント順序証明検証方法を説明するシーケンス図である。

[図17]図17は、本発明の第2の実施の形態に係るイベント順序証明システムの2ユーザ間の順序を判定する動作を説明するフローチャート図である。

[図18]図18は、本発明の第2の実施の形態に係るイベント順序証明システムの複合完全化によるルート値検証の動作を説明するフローチャート図である。

[図19]図19は、本発明の第2の実施の形態に係るイベント順序証明システムの補完データ完全化を説明する図である。

[図20]図20は、本発明の第2の実施の形態に係るイベント順序証明システムの補完データ完全化を説明する図である。

[図21]図21は、本発明の第3の実施の形態に係るイベント順序証明システムのシステム構成図である。

[図22]図22は、本発明の第3の実施の形態に係るイベント順序証明システムのイベント順序証明方法のイベント順序証明要求ステップを説明するシーケンス図である。

[図23]図23は、本発明の第3の実施の形態に係るイベント順序証明システムのイベント順序証明方法のイベント順序証明要求ステップを説明するシーケンス図である。

[図24]図24は、本発明の第3の実施の形態に係るイベント順序証明システムのイベント順序証明方法の監査用受理証明書受信ステップを説明するシーケンス図である。

[図25]図25は、本発明の第3の実施の形態に係るイベント順序証明システムのイベント順序証明検証方法の区間時刻証明書ステップを説明するシーケンス図である。

[図26]図26は、深さの違いを1以内に押さえ、ダミーノードを作成しない動的な順次集約木の構成方法を説明する図である。

[図27]図27は、インクリメンタルに順次集約木を構成する方法のアルゴリズムを説明する図である。

[図28]図28は、インクリメンタルに順次集約木を構成する方法のアルゴリズムを説明する図である。

[図29]図29は、インクリメンタルに順次集約木を構成する方法を説明する図である。

[図30]図30は、インクリメンタルに順次集約木を構成する方法において各ノードに値

を割付けるタイミングを説明する図である。

[図31]図31は、認証点の割当値は、監査点の受理証明書内補完データに含まれることを説明する図である。

[図32]図32は、認証点のレベルより低い認証パスノードは、遅延補完データあるいは受理証明書内補完データに含まれることを説明する図である。

[図33]図33は、認証点のレベルより低い認証パスノードは、遅延補完データあるいは受理証明書内補完データに含まれることを説明する図である。

[図34]図34は、本発明の第4の実施の形態に係るイベント順序証明システムのシステム構成図である。

[図35]図35は、本発明の第4の実施の形態に係るイベント順序証明システムに用いられる順次集約木の構成を説明する図である。

[図36]図36は、本発明の第4の実施の形態に係るイベント順序証明システムのイベント順序受理証明書の構成を示す図である。

[図37]図37は、本発明の第4の実施の形態に係るイベント順序証明システムにおいて各登録点とその補完データを説明する図である。

[図38]図38は、本発明の第4の実施の形態に係るイベント順序証明システムの利用者装置におけるイベント順序の判定方法を説明する図である。

[図39]図39は、本発明の第4の実施の形態に係るイベント順序証明システムのイベント順序証明方法の動作を説明するシーケンス図である。

[図40]図40は、本発明の第4の実施の形態に係るイベント順序証明システムのイベント順序証明検証方法の動作を説明するシーケンス図である。

[図41]図41は、本発明の第4の実施の形態に係るイベント順序証明システムのイベント順序証明検証方法の動作を説明するシーケンス図である。

[図42]図42は、本発明の第5の実施の形態に係るイベント順序証明システムのシステム構成図である。

[図43]図43は、本発明の第5の実施の形態に係るイベント順序証明システムのイベント順序受理証明書の構成を示す図である。

[図44]図44は、本発明の第5の実施の形態に係るイベント順序証明システムにおけ

る完全化波及処理を説明する図である。

[図45]図45は、本発明の第5の実施の形態に係るイベント順序証明システムにおいて完全化波及処理を用いることにより、連鎖補完方式の証明応答からシーケンス補完方式の証明応答を計算できることを示す図である。

[図46]図46は、本発明の第5の実施の形態に係るイベント順序証明システムにおいて第1の連鎖補完方式を説明する図である。

[図47]図47は、本発明の第5の実施の形態に係るイベント順序証明システムにおいて第1の連鎖補完方式による証明応答作成の動作を説明するフローチャートである。

[図48]図48は、本発明の第5の実施の形態に係るイベント順序証明システムにおいて第2の連鎖補完方式を説明する図である。

[図49]図49は、本発明の第5の実施の形態に係るイベント順序証明システムにおいて第2の連鎖補完方式による証明応答作成の動作を説明するフローチャートである。

[図50]図50は、本発明の第5の実施の形態に係るイベント順序証明システムの第2の連鎖補完方式におけるデータ構造の一例である。

[図51]図51は、本発明の第5の実施の形態に係るイベント順序証明システムの連鎖補完方式における即時補完データ及び遅延補完データの計算手順の一例を説明するフローチャートである。

[図52]図52は、本発明の第5の実施の形態に係るイベント順序証明システムの連鎖補完方式におけるノード値計算順の一例を説明するフローチャートである。

[図53]図53は、本発明の第5の実施の形態に係るイベント順序証明システムの連鎖補完方式における遅延データ設定手順の一例を説明するフローチャートである。

[図54]図54は、本発明の第5の実施の形態に係るイベント順序証明システムの連鎖補完方式における順次集約木の切替処理の一例を説明するフローチャートである。

[図55]図55は、本発明の第5の実施の形態に係るイベント順序証明システムの連鎖補完方式における順次集約木の終端・切替処理のサブルーチンの一例を説明するフローチャートである。

[図56]図56は、本発明の第5の実施の形態に係るイベント順序証明システムの連鎖補完方式における順次集約木の切替処理のサブルーチンの一例を説明するフロー

チャートである。

[図57]図57は、図55の処理を具体的に説明する図である。

[図58]図58は、順次集約フォレストと順次集約小木を説明する図である。

[図59]図59は、順次集約フォレストと現時点順次集約木を説明する図である。

[図60]図60は、本発明の第5の実施の形態に係るイベント順序証明システムの連鎖補完方式におけるインクリメンタル完全個別化の動作を説明するフローチャートである。

[図61]図61は、図60の処理を具体的に説明する図である。

[図62]図62は、本発明の第5の実施の形態に係るイベント順序証明システムの連鎖補完方式におけるインクリメンタル完全個別化の順次集約小木決定の計算手順の一例を説明するフローチャートである。

[図63]図63は、本発明の第5の実施の形態に係るイベント順序証明システムの連鎖補完方式におけるインクリメンタル個別完全化の取得参照点決定の計算手順の一例を説明するフローチャートである。

[図64]図64は、本発明の第5の実施の形態に係るイベント順序証明システムの連鎖補完方式におけるインクリメンタル個別完全化の連鎖補完データ蓄積用データ構造の一例である。

[図65]図65は、本発明の第5の実施の形態に係るイベント順序証明システムの連鎖補完方式におけるインクリメンタル個別完全化のアルゴリズムを説明する図である。

[図66]図66は、本発明の第5の実施の形態に係るイベント順序証明システムの連鎖補完方式におけるインクリメンタル個別完全化の認証パスノードの割当値の計算手順の一例を説明するフローチャートである。

[図67]図67は、本発明の第5の実施の形態に係るイベント順序証明システムの連鎖補完方式におけるインクリメンタル個別完全化の認証パスノードの各割当値の計算手順の一例を説明するフローチャートである。

[図68]図68は、本発明の第5の実施の形態に係るイベント順序証明システムの連鎖補完方式におけるインクリメンタル一括個別化の手順の一例を説明するフローチャートである。

[図69]図69は、本発明の第5の実施の形態に係るイベント順序証明システムの連鎖補完方式におけるインクリメンタル一括個別化の根拠を説明する図である。

[図70]図70は、本発明の第5の実施の形態に係るイベント順序証明システムの連鎖補完方式におけるインクリメンタル一括個別化の根拠を説明する図である。

[図71]図71は、本発明の第5の実施の形態に係るイベント順序証明システムの連鎖補完方式におけるインクリメンタル完全化(一部をメモリに納め、多段式に実行する方式)を説明する図である。

[図72]図72は、本発明の第5の実施の形態に係るイベント順序証明システムの連鎖補完方式におけるインクリメンタル完全化(一部をメモリに納め、多段式に実行する方式)を説明する図である。

[図73]図73は、本発明の第5の実施の形態に係るイベント順序証明システムの連鎖補完方式におけるインクリメンタル完全化(一部をメモリに納め、多段式に実行する方式)を説明する図である。

[図74]図74は、本発明の第5の実施の形態に係るイベント順序証明システムの連鎖補完方式におけるインクリメンタル完全化(一部をメモリに納め、多段式に実行する方式)を説明する図である。

[図75]図75は、本発明の第5の実施の形態に係るイベント順序証明システムの連鎖補完方式におけるインクリメンタル完全化(一部をメモリに納め、多段式に実行する方式)を説明する図である。

[図76]図76は、完全認証パスデータによる順次集約木のルート値の計算方法を示すフローチャートである。

[図77]図77は、ある集約間隔の順次集約木のリーフの1つとして、前の集約間隔の順次集約木のルート値を取り入れる場合の順次集約木を説明する図である。

[図78]図78は、ある集約間隔の順次集約木のリーフの1つとして、前の集約間隔の順次集約木のルート値を取り入れる場合の順次集約木を説明する図である。

[図79]図79は、ある集約間隔の順次集約木のリーフの1つとして、前の集約間隔の順次集約木のルート値を取り入れる場合の完全認証パスデータによる順次集約木のルート値の計算方法を説明する図である。

[図80]図80は、認証点の割当値は、監査点の受理証明書内補完データに含まれることを説明する図である。

[図81]図81は、認証点の割当値は、監査点の受理証明書内補完データに含まれることを説明する図である。

[図82]図82は、認証点のレベルより低い認証パスノードは、遅延補完データあるいは受理証明書内補完データに含まれることを説明する図である。

[図83]図83は、認証点のレベルより低い認証パスノードは、遅延補完データあるいは受理証明書内補完データに含まれることを説明する図である。

[図84]図84は、認証点のレベルより低い認証パスノードは、遅延補完データあるいは受理証明書内補完データに含まれることを説明する図である。

[図85]図85は、認証点のレベルより低い認証パスノードは、遅延補完データあるいは受理証明書内補完データに含まれることを説明する図である。

発明を実施するための最良の形態

[0022] 以下、本発明の実施の形態を図面を用いて説明する。

[0023] ＜第1の実施の形態＞

(1－1. システム構成)

図3は、本発明の第1の実施の形態に係るイベント順序証明システム100のシステム構成図である。イベント順序証明システム100は、イベント順序証明装置(以下、証明装置という)1、複数のイベント順序証明利用者装置(以下、利用者装置という)2i(i=a, b, …,n)、証明装置1が発行したイベント順序受理証明書(以下、受理証明書という)の監査を行うイベント順序証明監査装置(以下、監査装置という)3、及び、以上の各装置を相互に接続する、例えば、インターネット網、電話回線網などにより構成されるコンピュータネットワーク4を備えており、証明装置1が利用者装置2iからのイベント順序証明要求(以下、証明要求という)に応えて、受理証明書を発行し、利用者装置2iに返信すると共に、受理証明書に疑義が生じた場合には、利用者装置2iは、証明装置1が公表したデータ又は監査装置3による監査結果によって受理証明書を検証することができるようになっている。

[0024] 尚、イベント順序証明システム100のシステム構成は機能が同一であればその形態

は問わないものであり、その物理的構成は種々考えられるものである。例えば、図4に示すように、利用者装置2iの代わりに、イベント順序証明利用者検証装置(以下、利用者検証装置という)6iが受理証明書の検証を行うようにしてもよいし、証明装置1の代わりに電子的情報公表装置5が証明装置1から公表データをもらい、公開するようにしてもよい。また、コンピュータネットワーク4は、郵便など他の通信手段に置き換えることも可能である。尚、以下においては、図3のシステム構成のもとに構成及び動作を説明する。

[0025] 証明装置1は、コンピュータネットワーク4を介して利用者装置2i及び監査装置3とデータの送受信を行う送受信部11、利用者装置2iからの証明要求として送信されたデジタル・データを順次集約木を用いてまとめるイベント順序証明要求集約部12、受理証明書を作成するイベント順序証明作成部13、監査装置3に送信する監査情報を作成する監査情報作成部14、利用者装置2iからの補完データ要求に応えて補完データを取得する補完データ取得部15、証明装置1が一定期間に発行した複数の受理証明書の内容を連結したデータに対して高強度デジタル署名をするデジタル署名作成部16、高強度デジタル署名されたデータを電子的に公表する電子的情報公表部17、及び受理証明書をはじめとするイベント順序証明に関する情報を記憶する記憶部18を有する構成である。

[0026] 上述したように、イベント順序証明要求集約部12は、順次集約木を用いてイベント順序証明要求をまとめるが、この順次集約木について図5を用いて説明する。図5に示す順次集約木は、一定期間(例えば1週間など証明装置1が取り纏めデータを公表するサイクル、以下、順次集約期間という)において完成される集約木であって、利用者装置2iからの証明要求に含まれるデジタル・データの全部あるいは一部から所定の順次割当データ計算手順に従って生成されたデジタル・データ(これを順次割当データと呼ぶ;例えば、証明要求に含まれるデジタル・データのハッシュ値)を経時的に順次リーフに左側から割り当てるようにしている。

[0027] 順次集約木の各ノード(リーフを除く)に割り当てられる値の計算方法は、以下の通りである。順次集約木の親の割当値は、左側の子の割当値H'と右側の子の割当値H"を連接(ビット列とビット列の結合)し、所定の衝突困難一方向ハッシュ関数hを適用

した結果であるハッシュ値を計算することにより求められるものであり、これをh(H' ‖ H")と表す。このようにして下位のレベルの割当値から上位のレベルの割当値を計算して、最終的に最上位のレベル(ルート)の割当値(ルート値)を求める。

[0028] 以下においては、図5に示すように、16個のリーフを有する順次集約木の場合について説明する。尚、順次集約木リーフの数や高さは、順次集約期間が終了するまで確定しない。また、順次集約木においては、リーフへの値の割当は左から順次行われ、レベルが0より大きいノード(即ちリーフではないノード)に対する値の割当は、それが可能になったときにインクリメンタルに行われる。従って、図3の同一の縦線上にある複数のノードに対しては、値の割当が同一の処理単位の中でほぼ同時に行われる。

ここで、順次集約木のレベルj、番号(インデックスともいう)iのノードを(j, i)で表し、ノード(j, i)の割当値をV(j, i)と表して、図5に示す具体例を説明する。

[0029] 今、順次割当データがノード(0,5)に割り当てられたとき、即ち、順次集約木リーフに割り当てるハッシュ値がV(0,5)であるとき、このハッシュ値V(0,5)からルート値(= V(4,0))を求めるには、V(0,5)にV(0,4)を左から連接して、ハッシュ値h1'を計算し、該ハッシュ値h1'にV(1,3)を右側から連接してハッシュ値h2'を計算し、該ハッシュ値h2'にV(2,0)を左側から連接してハッシュ値h3'を計算し、さらに該ハッシュ値h3'にV(3,1)を右側から連接してハッシュ値(= V(4, 0))を計算すればよい。このような手順によりV(0,5)とそれを補完するデータ(ここではV(0, 4), V(1,3), V(2,0), V(3,1))からルート値が計算できるとき、V(0, 5)はハッシュ関数hによりルート値にリンクするという。また、順次集約木におけるV(0,5)の補完データ(以下、順次集約補完データという)は、

[(V(0, 4), L), (V(1, 3), R), (V(2, 0), L), (V(3, 1), R)]

となる。ここで、L及びRは、各々、2つのデジタル・データを連接する際に左から連接こと、及び右から連接することを表す。

[0030] イベント順序証明作成部13は、図6に示すような受理証明書EOC(y)を作成し、利用者装置2iに送信するようになっている。受理証明書EOC(y)は、利用者から送付されたデジタル・データy、上述した順次割当データ計算手順によりデジタル・データyから計算された順次割当データz、順次割当データzが割当てられた順次集約木を一意

に特定できる順次集約木番号、順次割当データzが割当てられた順次集約木リーフを一意に特定できる順次集約木リーフ番号、およびその時点で取得できる順次集約補完データの一部(これを即時補完データという)HKを含むように構成されている。このうち、即時補完データHKについては省くことも可能である。

[0031] また、イベント受理証明書EOC(y)には、証明装置1が予め用意しておいた公開鍵暗号方式キー・ペアのうちの秘密鍵(署名用秘密鍵)を用いてデジタル署名をつけて送信してもよい。この場合、当該公開鍵暗号方式キー・ペアのうちの公開鍵は公開鍵暗号基盤などを用いて利用者装置2iからアクセス可能になっているものとする。

[0032] 尚、当該の受理証明書EOC(y)発行後に取得できる順次集約補完データを遅延補完データという。即ち、受理証明書EOC(y)が作成される段階においては、即時補完データだけが利用者装置2iに送信されるものであり、遅延補完データは、当該の受理証明書EOC(y)発行後に要求された場合等に利用者装置2iに送信されるものである。例えば、図5においては、ノード(0,5)にとって、ノード割当値V(2,0)、ノード割当値V (0,4)は即時補完データであるが、ノード割当値V (1,3)、ノード割当値V (3,1)はノード(0, 15)が割当られた時点以降に取得可能な遅延補完データである。以下では、順次集約木リーフ番号 i に対して、V(0, i) のことを短くV(i)と書くこともある。

[0033] 補完データ取得部15は、利用者装置2iから上述した遅延補完データの要求があったとき、当該時点に関する情報(当該要求が割り当てられた順次集約木番号、順次集約木リーフ番号)、及びその時点で確定している順次集約補完データ(位置情報、割当値)の全てを利用者装置2iに返送するようになっている。

[0034] ここで、図7を参照して、順次集約補完データの内容について詳しく説明する。

[0035] 順次集約木の1つのリーフtに対する、tより右に位置するもう一つのリーフt'における補完データCToken(t, t')は次のように定義される。

[0036] リーフtから順次集約木のルートに至るパスをtのルート・パスと呼び、tのルート・パスに属するルート以外のノードの兄弟ノードからなるノードの並びをtの認証パスと呼ぶ(認証パスの詳細な定義は後で与える)。認証パスの要素の内、tより右に位置するリーフt1の割り当て値が確定した時点において割当値が確定している要素の列をauthPathD(t, t1)とし、これをt1におけるtに対する認証パスと呼ぶ。この列に割当値の情

報を付加したものをauthPathDV(t, t1)とし、これをt1におけるtに対する値付認証パスと呼ぶ。

[0037] 以上から、authPathDV(t, t')は、受理証明書EOC(y)に含まれていなかった情報を含めて、補完データCToken(t, t')を構成するようになっている。

[0038] 尚、t'がtの属する順次集約木SBTの生成期間(順次集約期間)の終了後に生成される次の順次集約木SBT'のリーフであるときにも、authPathDV(t, t')には順次集約木SBTについての情報のみが含まれる。このとき、CToken(t, t')は、t時点で受信したイベント受理証明書EOC(y)と組み合わせることにより、当該の順次集約期間における順次集約木のルート値を計算するのに十分な情報を含んでいる。

[0039] 例えば、図7において、CToken(t, t4')はa1の位置情報(0, 3)とその割当値V(a1)の組((0, 3), V(a1)) 、及びa2 の位置情報(2, 1)とその割当値 V(a2)の組((2, 1), V(a2))からなる列[((0, 3), V(a1)), ((2, 1), V(a2))] となる。

[0040] 以下では、受理証明書に含まれる順次集約木の割当て値と組み合わせることにより前記順次集約木のルート値を計算できるような補完データを該受理証明書の完全補完データと定義し、上記割当て値および受理証明書に含まれる即時補完データと組み合わせることにより、前記順次集約木のルート値を計算できるような補完データを完全遅延補完データと呼ぶ。

[0041] 監査情報作成部14は、監査情報を順次集約木から取得して監査装置3に送信するものであり、より詳しくは、監査情報とは、順次集約木リーフに設けられた監査点において以下に定義するように生成される監査用イベント順序受理証明書(以下、監査用受理証明書という)から構成される。ここで、監査点とは、監査装置3からの監査用イベント順序証明要求(以下、監査用証明要求という)が割当てられた順次集約二分木のリーフをいう。

[0042] 尚、図5においては、監査点は1つしか設けられていないが、所定のアルゴリズムに従って複数設けてよいのは勿論であり、また、証明要求に対する受理証明書に対して後述するような監査を行うためには、監査点は、該証明要求に対応するリーフ(図3の具体例においては、ノード(0, 5))に等しいか或いはそれより右側のリーフ(時間的に後)に割り当てられていればどこに設けていてもよいものである。

[0043] 監査用受理証明書の形式は、利用者装置2iに返送する受理証明書と同一である。尚、順次割当データを計算するための元となるデジタル・データyは、監査装置3から証明装置1に監査用証明要求として送付されたものであってもよいし、当該証明装置1において、当該の監査装置2に対して予め定められた何らかの手順に従って生成してもよい。また、このような手順としては、前以て定められた何らかの手順に従って監査用受理証明書におけるイベント順序証明の対象となるデジタル文書を作成し、該デジタル文書に対して前以て定めたハッシュ関数を適用した結果であるハッシュ値を順次割当データを計算するための元となるデジタル・データとする方式を採用してもよい。

[0044] 利用者装置2iは、コンピュータネットワーク4を介して証明装置1および監査装置3とデータを送受信する送受信部21、所定のデジタル・データを含む証明要求を行うイベント順序証明要求部22、要求時点において取得可能な受理証明書に対する補完データを要求する補完データ要求部23、受理証明書を検証するイベント順序証明検証部24、受理証明書をはじめとするイベント順序証明に関する情報を記憶する記憶部25を有する構成である。

[0045] ここで、イベント順序証明検証部24は、受理証明書に対して以下の検証機能を備える。

[0046] まず、受理証明書にデジタル署名が含まれる場合には、該デジタル署名に対するデジタル署名検証を行う第0の検証機能を備える。

[0047] また、証明装置1から高強度デジタル署名を付すこと等により真正性を保証して公表される公表情報に、受理証明書に含まれる順次割当データがハッシュ関数を介してリンクすることを検証する第1の検証機能を備える。

[0048] さらに、以下に記述するように、証明装置1からの公表情報が公開される前であっても、監査装置3を利用することにより、受理証明書の正当性を検証する第2の検証機能を備える。

[0049] 監査装置3は、コンピュータネットワーク4を介して証明装置1および利用者装置2iとデータを送受信する送受信部31、利用者装置2iからある受理証明書の監査要求を受けた際には、利用者装置2iから送信された監査要求情報および自己の監査情報

を用いて受理証明書の検証を行い、その結果を利用者装置2iに返信するイベント順序証明監査部32、及び監査用受理証明書をはじめとする監査情報を記憶する記憶部33を有する構成である。

[0050] ここで、イベント順序証明検証部32の機能について、図5を用いて説明する。図5においては、(0, 10)が監査点となっているので、この時点において監査装置3が受け取っている監査情報は、上述した通り、V(3, 0)およびV(1, 4)である。一方、利用者装置2iは、監査要求情報として、V(0, 5)及び順次集約補完データであるV(0, 4), V(1, 3)、およびV(2, 0)を送信するものである。これは、利用者装置2iが検証を求める時点(即ち、受理証明書が発行された(0, 5)の時点より後刻である監査点(0, 10)の時点以降)においては、即時補完データに含まれていなかったV(1,3)も証明装置1から取得することが可能であるので、V(1, 3)を遅延補完データとして利用者装置2iが証明装置1から取得し、監査要求情報に含めたものである。そして、イベント順序証明検証部32は、自己が有している監査情報V(3, 0)が、利用者装置2iから送信された監査要求情報から計算されたV(3, 0)と一致するか否かを検証するものである。

[0051] 尚、以後においては、利用者装置2iから送信された証明要求から作成された順次割当データが割り当てられた順次集約木リーフをユーザ点と呼び、監査装置3から送信された監査用証明要求から作成された順次割当データが割り当てられた順次集約木リーフを監査点と呼ぶ。

[0052] ここで、比較検証の対象となる順次集約木のノード(図5においては、(3, 0))を以後、認証点とよぶ。尚、一般に、あるユーザ点の番号が監査点の番号より小さい場合、認証点のラベル(割当値)は監査情報に含まれており、また、監査点におけるイベント順序証明処理が終了した時点以降において、利用者装置2iが受信できる遅延補完データから計算できるラベルには、認証点のラベルが含まれるので、順次集約木においてユーザ点、監査点、遅延補完データを要求した点が左からこの順序に位置している場合には、上記検証は、常に実施可能なものであるが、この理由に関しては後述する(後述の順次集約木の性質2の項目(3)を参照)。

[0053] 即ち、上記の手順により利用者装置2iがある受理証明書に対する第2の検証を監査装置3に依頼して実行するには、該受理証明書の証明要求が割り当てられたリー

フτと、該イベント受理証明書に対する遅延補完データ要求が割り当てられたリーフτ'の間(τとτ'も含む)に監査装置3の監査点が存在する必要がある。

[0054] 尚、以上の各装置は、少なくとも演算機能及び制御機能を備えた中央処理装置(CPU:Central Processing Unit)、プログラムやデータを収納する機能を有するRAM(Random Access Memory)等からなる主記憶装置(メモリ)、ハードディスク(HD)等の電源断時にもデータを記憶し続けることが出来る2次記憶装置を有する電子的な装置から構成されている。このうち、証明装置1のイベント順序証明要求集約部12、イベント順序証明作成部13、監査情報作成部14、補完データ取得部15、デジタル署名作成部16及び電子的情報公表部17、利用者装置2iのイベント順序証明要求部22、補完データ要求部23及びイベント順序証明検証部24、並びに監査装置3のイベント順序証明監査部32の処理は、上記CPUによる演算制御機能を具体的に示したものに他ならない。また、証明装置1の記憶部18、利用者装置2iの記憶部25及び監査装置3の記憶部33は、上記主記憶装置あるいは2次記憶装置の機能を備えたものである。

[0055] また、本実施の形態に係る各種処理を実行するプログラムは、前述した主記憶装置または2次記憶装置に格納されているものである。そして、このプログラムは、ハードディスク、フレキシブルディスク、CD－ROM、MO、DVD－ROMなどのコンピュータ読み取り可能な記録媒体に記録することも、通信ネットワークを介して配信することも可能である。

[0056] (1－2. システム動作)

次に、以上の構成を有するイベント順序証明システム100におけるイベント順序証明方法、およびイベント順序証明検証方法を図8乃至10を用いて説明する。ここで、図8は、1つの順次集約期間において証明装置1が受理証明書及び監査用受理証明書を作成する動作を説明するシーケンス図であり、図9は、利用者装置2iが受理証明書に対して第1の検証を行う動作を説明するフローチャートであり、図10は、利用者装置2iが受理証明書に対して第2の検証を行う動作を説明するシーケンス図である。

[0057] まず、図8を参照して、イベント順序証明方法について説明する。

[0058] 利用者装置2iが証明装置1にデジタル・データy を含む証明要求を送信すると、証

明装置1は送受信部11を介して、該デジタル・データyを含む証明要求を受信する(ステップS10, S20)。

次に、イベント順序証明要求集約部12が、デジタル・データy を入力の一部あるいは全部として順次割当データzを計算し、該順次割当データzを順次集約木リーフに割り当て、インクリメンタルに順次集約木を構成していくとともに、イベント順序証明作成部13が、受理証明書EOC(y)を作成し、送受信部11を介して利用者装置2iに受理証明書EOC(y)を送信する(ステップS30, S40, S50)。

[0059] これにより、利用者装置2iは、受理証明書EOC(y)を取得することができる(ステップS60)。尚、受理証明書EOC(y)には、この時点において取得できる即時補完データを含めることにしてよいが、遅延補完データは含まれていない。

[0060] 同様にして、監査装置3も監査用証明要求を送信すると、証明装置1は送受信部11を介して、監査用証明要求を受信する(ステップS70, S80)。

[0061] 次に、イベント順序証明要求集約部12が、監査用証明要求から計算された監査用順次割当データを順次集約木リーフに割り当てて、インクリメンタルに順次集約木を構成していくとともに、監査情報作成部13は、監査用受理証明書を作成し、送受信部11を介して監査装置3に監査用受理証明書を送信する(ステップS90, S100, S110)。

[0062] これにより、監査装置3は、監査用受理証明書を取得することができる(ステップS120)。

[0063] 次に、利用者装置2iは、取得した受理証明に対する遅延補完データ要求を証明装置1に送信すると、証明装置1は送受信部11を介して、該遅延補完データ要求を受信する(ステップS130, S140)。

[0064] 次いで、証明装置1の補完データ取得部15は、その時点で取得可能な上記受理証明書に対する補完データを取得し、遅延補完データとして送受信部11を介して利用者装置2iに送信する(ステップS150, S160)。

[0065] これにより、利用者装置2iは、監査に必要な遅延補完データを取得することができる(ステップS170)。

[0066] そして、順次集約のための一定期間(順次集約期間)内においては、上述した証明

装置1の動作は繰り返され、順次集約期間が終了すると、順次集約木のルート値 を計算し、電子的情報公表部17は、このルート値を電子的に公表する(ステップS180, S190, S200)。この際、該情報の真正性を保証するため、高強度デジタル署名作成部16を用いて高強度のデジタル署名を付した公表情報を公開してもよい。

[0067] 尚、図8に示すイベント順序証明方法においては、監査装置3の方から証明装置1に監査情報要求を送信し、これに応えて証明装置1が監査装置3に監査情報を送信する方式であったが、これとは異なり、証明装置1が監査装置3に監査情報を自動的に送信するような方式であってもよい。

[0068] 次に、図9を参照しながら、電子的に公表された公表情報を用いたイベント順序証明検証方法について説明する。これは、利用者装置2iの第1の検証機能に相当するものである。

[0069] まず、利用者装置2iは、自己が証明装置1に証明要求として送信したデジタル・データy、並びに受信した受理証明書EOC(y)及び遅延補完データに含まれている順次集約補完データ(この時点においては、すべての順次集約補完データを取得可能である)から順次集約木のルート値RHcalを計算する(ステップS310)。

[0070] 次に、高強度のデジタル署名を付して電子的に公表されている同一順次集約期間のルート値RHを取得し、このルート値RHが、計算したルート値RHcal に一致するか否か検証する(ステップS320, S330)。

[0071] 以上の検証において、検証に成功すれば、受理証明書が改ざんされていないことを確認することができる(ステップS340)。一方、検証に失敗すれば、受理証明書が改ざんされていることを確認することができる(ステップS350)。これにより、高強度のデジタル署名を付すなどの手段により真正性を保証しながらが電子的に公表された後においては、公表された情報を利用して、証明装置1が発行した受理証明書が、当該の順次集約期間において、受理証明書に含まれる元デジタル・データに対して、受理証明書に含まれる順次集約木リーフ番号で識別される順番において発行されたものであることを確実に検証することができる。

[0072] 次に、図10を参照しながら、監査装置3を用いたイベント順序証明検証方法について説明する。これは、利用者装置2iの第2の検証機能に相当するものである。

[0073] 利用者装置2iは、監査要求の前に検証の対象となる受理証明書の遅延補完データを証明装置1に要求する(ステップS410)。この要求を証明装置1が送受信部11を介して受信すると、補完データ取得部15は、受理証明書に即時補完データが含まれる場合には、この時点において取得できる遅延補完データの全てから即時補完データを除いたものからなる遅延補完データを、受理証明書に即時補完データが含まれない場合には、この時点において取得できる遅延補完データの全てを取得し、送受信部11を介して利用者装置2iに送信する(ステップS420, S430, S440)。これにより、利用者装置2iは、補完データを取得するので、イベント順序証明検証部24は、これに既に受け取っている受理証明書を加えた監査要求情報を監査装置3に送信する(ステップS450, S460)。

[0074] 次に、監査装置3が監査要求情報を送受信部31を介して受信すると、イベント順序証明監査部32は、既に自分が受信した監査用受理証明書が割当てられた順次集約木のリーフの中で、受信したこの監査要求情報に含まれる受理証明書が割当てられた順次集約木リーフτとその遅延補完情報に含まれるリーフτ'の間にある監査点αを計算する(ステップS470, S480)。続いて、監査要求情報からτのαによる認証点を計算し、該認証点の割当値Acalを計算する(ステップS490)。一方、イベント順序証明検証部32は、監査情報として既に受け取っているこの認証点の割当値Aを記憶部33から取得して、この認証点の割当値Aが、計算により求めた認証点の割当値Acalに一致するか否かを検証する(ステップS500, S510)。

[0075] 以上の検証において、検証に成功すれば、受理証明書が改ざんされていないことを確認することができる(ステップS520)。一方、検証に失敗すれば、受理証明書が改ざんされていることを確認することができる(ステップS530)。そして、イベント順序証明監査部32は、この監査結果を送受部31を介して利用者装置2iに送信し、利用者装置2iは、監査結果を受信する(ステップS540, S550)。

[0076] これにより、利用者装置2iは、電子的公表機関を介した公表前においても、証明装置1が発行した受理証明書が当該の順次集約期間において、受理証明書に含まれる元デジタル・データに対して、受理証明書に含まれる順次集約木リーフ番号で識別される順番において発行されたものであることを確実に検証することができる。尚、

上記監査結果に監査点αの識別子を含めてもよい。この場合においては、利用者装置2iは、上記監査を要求した受理証明書に対応する証明要求の登録が、監査点αに対応する監査用証明要求の登録より前であったことの保証を監査装置3から確実に得ることができる。

[0077] なお、ステップS540の監査結果の送信に際しては、監査装置3が受信した補完データを含む部分に対して、証明監査装置3が持つ署名用秘密鍵を用いてデジタル署名を付して、該デジタル署名を含めた検証結果を構成し、利用者装置2iに送信するようにしてもよい。これにより、監査装置3によるデジタル署名が信用されるという前提の下で、順次集約木のルート値に対する有効なデジタル署名が入手できない場合であっても、利用者装置2iを利用する利用者は、上記受理証明書によるイベント順序証明の正当性を客観的に第三者に証明することができるようになる。

[0078] (1－3．イベント順序監査方法)

次に、上述した第2の検証である監査装置3を用いたイベント順序証明検証方法について、より詳しく説明する。

[0079] 尚、以下では、時刻の原点として、イベント順序証明システム100のサービス開始時点をとり、時間を計る単位として一つの値(例えば1秒、1ミリ秒等)を定め、時刻を上記原点から上記の時間の単位で計った整数で表現するものとする。

[0080] ここで、イベント順序証明検証方法を説明するための幾つかの予備定義を与える。

[0081] 順次集約木SBTにおいて、1つのノードpはレベルjとレベル内の番号iで識別されるが、ノードpのレベルと番号を各々level(p), index(p)と書く。

[0082] また、順次集約木リーフ番号iで識別される順次集約木SBTのリーフをleaf(SBT, i), leaf(SBT, i)に順次割当値を割り当てる元となった証明要求を受付けて該リーフに割当値を割り当てる一連の処理を該リーフに対する処理ラウンドと言い、round(SBT, i)と表す。文脈からどの順次集約木について論じているか明らかなときは、単にleaf(i), round(i)と記すこともある。

[0083] 順次集約木には、生成された順に0から始まる識別番号を付与し、これを順次集約木番号という。n番目の順次集約木リーフの数をN(n)とおく。

[0084] 各受理証明書に対しては、順次集約木番号nと順次集約木リーフ番号iが付与され

、該受理証明書が発行された順次集約木リーフをそれら2つの番号の組で指定することができる。このような組を拡張リーフ識別子と呼ぶ。2つの拡張リーフ識別子 $\nu 1 = (n1, i1)$, $\nu 2 = (n2, i2)$の間の順序を辞書式順序を用いて定義する。即ち、$\nu 1 < \nu 2$とは、$n1 < n2$、または$n1 = n2$ かつ $i1 < i2$ のことと定義する。また $\nu 1 \leqq \nu 2$とは、$\nu 1 < \nu 2$または$\nu 1 = \nu 2$のことと定義する。$\nu = (n, i)$ を拡張リーフ識別子とし、この識別子で識別される順次集約木リーフがあるとき、該リーフを $leaf(\nu) = leaf(n, i)$と表す。$leaf(\nu)$を単に、リーフνと呼ぶこともあり、$leaf(\nu)$が監査点(あるいはユーザ点)であるときは、監査点 ν (あるいはユーザ点 ν)と呼ぶこともある。

[0085] また、ある順次集約木SBTのリーフleaf(SBT, i)について、この順次集約木SBTのリーフに順次割当値を割り当てる元となった証明要求の受付時刻を、該リーフに対応する時刻といい、これをtime(SBT, i)あるいは簡単にtime(i)と表す。同様に、$leaf(\nu)$について、このリーフに順次割当値を割り当てる元となった証明要求の受付時刻を、time(ν)と表す。

[0086] 利用者装置2iが、監査装置3を用いて、ある受理証明書に対する第2の検証を実行するには、上述したように該受理証明書に対応する順次集約木リーフτと、該受理証明書に対する遅延補完データ要求に対応する順次集約木リーフτ'の間(τとτ'も含む)に監査装置3の監査点αが存在する必要がある。このためには、Tをある正整数とし、以下の3つの条件(1)～(3)が成り立てば十分である。

[0087] (1)監査装置3の最初の監査点の時刻はTより小さい。

[0088] (2)監査装置3による任意の1つの監査点をα、次の監査点をα'とすると、

$$time(\alpha') - time(\alpha) \leqq T$$

が成り立つ。

[0089] (3) 利用者装置2i は、拡張リーフ識別子 τ の順次集約木リーフで受理証明書を受信した後のある順次集約木リーフτ'で該受理証明書に対する遅延補完データを受信することとし、

$$time(\tau') - time(\tau) \geqq T$$

が成り立つ。

[0090] 尚、これらの条件の十分性の理由に関しては後述する(後述の次集約木の性質3の

(1)と(2)を参照)。

[0091] 図11に示すようなある順次集約木SBTに属する監査装置3の監査点αにおいて、監査装置3は監査用受理証明書を受信するものとする。監査用受理証明書には、αにおける即時補完データが含まれている。この即時補完データには、順次集約木SBTの任意のリーフτでαより左にあるものの割当値V(τ)が次のような意味で結合している。即ち、τのαによる認証点p2の割当値V(p2)が上記の即時補完データに含まれ、この認証点の割当値はV(τ)から出発してauthPath(τ)に属する幾つかのノードの割当値をハッシュ関数hによりリンクすることにより計算できる(これが成立つ理由については、後述の順次集約木の性質2の項目(1)を参照)。

[0092] これにより、監査装置3は監査点αで受信した監査用受理証明書内の即時補完データに、上記V(p2)が含まれているか否かにより、利用者がユーザ点τで取得した受理証明書の元となった要求の送信及び証明装置1による要求受付けが、監査装置3が監査点αで取得した監査用受理証明書の受信より時間的に前であることを検証することができる(これを検証結果1とする。図12を参照)。

ここで、証明装置1の直列化可能性について説明する。証明装置1の直列化可能性とは、該証明装置が任意の複数の順序証明要求を受付け処理する際に、該複数の要求を直列に並べるある順序付けがあり、その順序に従って順次受けて、それに対する処理結果である受理証明書を返信し、その後次の要求の処理を行った場合と同じ結果となることと定義する。

[0093] 証明装置の直列化可能性は重要な要件であり、本実施の形態においては、直列化可能性を保証する手段を有するものとする。このような手段としては、証明装置が1つ順序証明要求を受付けたとき、該要求に対する受理証明を送信してからのみ次の要求受付けることを監視する直列性監査装置を用いてもよい。

[0094] この直列化可能性を用いれば、ユーザ点と監査点の順序関係について検証結果1より強いことを結論することができる。例えば、順序証明装置1の直列化可能性が、監査装置3が監査点αで取得した受理証明書の受信時まで保証されていたとすると、上記検証により、ユーザ点τに対応する順序証明要求の受付けが、監査点αに対応する監査用順序証明要求の受付けより時間的に前であることを結論できる(これを

検証結果2とする。図12を参照)。なぜならば、直列化された順序証明要求の処理において、αに対応する監査用順序証明要求の受付けがτに対応する監査用順序証明要求の受付けより前であれば、αに対応する受理証明書EOC(α)は、τに対応する監査用順序証明要求EOR(τ)の受付けより前に送信されることになり、EOC(α)にEOR(τ)が含むイベント値がハッシュ関数を介して結合するデータを含めることは出来ないからである。以上から、監査装置3が監査点αで取得した監査用受理証明書の受信時まで、証明装置1の直列化可能性が推認されるときには、ユーザ点τに対応する順序証明要求の受付けは、監査点αに対応する監査用順序証明要求の受付けより時間的に前であることが推認される。以後、このことを「ユーザ点の未来側の境界付け」という。

[0095] 尚、監査装置3が監査点αで取得した監査用受理証明書の受信時までの証明装置1の直列化可能性を保証しても、監査装置3が受理証明の一部として即時補完データを受信していなければ、上記のことは言えないことに注意する必要がある。なぜならば、監査装置3が監査点αで取得した監査用受理証明書の受信時より後に、証明装置がτにおける割当て値を改変する可能性を除くことはできないからである。

[0096] 従って、第1の実施の形態のイベント順序証明システム100によれば、利用者装置2iから証明要求を受付けた証明装置1が、該要求に含まれるデジタル・データから計算される順次割当値及び前記順次割当データが割り当てられた順次集約木の位置情報を含む受理証明書及び補完データを発行し、補完情報順次集約木のルート値に対して高強度デジタル署名を付す等の手段により真正性を保証しながら電子的に公表するので、利用者装置2iは公表情報および補完データから簡単に受理証明書の検証をすることができる。また、順次集約木のルート値を電子的に公表する前であっても、監査装置3が順次集約木の監査点に関する監査情報を有しているので、監査装置5は利用者装置2iからの監査要求を受けて、受理証明書の監査をすることができる。

[0097] この結果、受理証明書の正当性を検証できたときには、証明装置1における監査対象とした受理証明書の証明要求受信が、監査に用いた監査用受理証明書の証明要求受信よりも時間的に前であることを証明することができる。

[0098] ＜第2の実施の形態＞

(2－1．システム構成)

図13は、本発明の第2の実施の形態に係るイベント順序証明システム200のシステム構成図である。イベント順序証明システム200は、イベント順序証明装置(以下、証明装置という)7、複数のイベント順序証明利用者装置(以下、利用者装置という)2i(i=a,b, …,n)、証明装置7が発行したイベント順序受理証明書(以下、受理証明書という)の監査を行うイベント順序証明監査装置(以下、監査装置という)8、及び、以上の各装置を相互に接続する、例えば、インターネット網、電話回線網などにより構成されるコンピュータネットワーク4を備えており、証明装置7が利用者装置2iからのイベント順序証明要求(以下、証明要求という)に応えて、受理証明書を発行し、利用者装置2iに返信すると共に、受理証明書に疑義が生じた場合には、利用者装置2iは、証明装置7が公表したデータ又は監査装置8による監査結果によって受理証明書を検証することができるようになっている。

[0099] ここで、第2の実施の形態は、第1の実施の形態とほぼ同様のシステム構成であるが、監査装置8が、各順次集約期間の終了後に、その順次集約期間中に取得した各監査用受理証明書の完全遅延補完データを、証明装置7に要求して(あるいは事前の契約に基づいて)取得するという点が異なっている。尚、本実施の形態においては、第1の実施の形態と異なる構成及び機能を説明し、その他の構成及び機能に関しては同一部分には同一符号を付して説明を省略する。

[0100] また、第1の実施の形態と同様に第2の実施形態においても、イベント順序証明システム200のシステム構成は機能が同一であればその形態は問わないものであり、その物理的構成は種々考えられるものである。例えば、利用者装置2iの代わりに、図4に示した利用者検証装置6iが受理証明書の検証を行うようにしてもよいし、証明装置7の代わりに、図4に示した電子的情報公表装置5が証明装置7から公表データをもらい、公開するようにしてもよい。また、コンピュータネットワーク4は、郵便など他の通信手段に置き換えることも可能である。

[0101] 証明装置7は、コンピュータネットワーク4を介して利用者装置2i及び監査装置8とデータの送受信を行う送受信部11、利用者装置2iからの証明要求として送信されたデ

ジタル・データを順次集約木を用いてまとめるイベント順序証明要求集約部12、受理証明書を作成するイベント順序証明作成部13、監査装置8に送信する監査情報を作成する監査情報作成部71、利用者装置2iからの補完データ要求に応えて補完データを取得する補完データ取得部15、証明装置7が一定期間に発行した複数の受理証明書の内容を連結したデータに対して高強度デジタル署名をするデジタル署名作成部16、高強度デジタル署名されたデータを電子的に公表する電子的情報公表部17、及び受理証明書をはじめとするイベント順序証明に関する情報を記憶する記憶部72を有する構成である。

[0102] 監査情報作成部71は、各監査点における監査用受理証明書を順次集約木から取得して作成することに加えて、各順次集約期間の終了後に、その順次集約期間に取得した各監査用受理証明書の完全遅延補完データを取得して作成するようになっている。

[0103] 監査装置8は、コンピュータネットワーク4を介して証明装置7および利用者装置2iとデータを送受信する送受信部31、証明装置7に各監査用受理証明書の完全遅延補完データの要求を行う補完データ要求部81、利用者装置2iからある受理証明書の監査要求を受けた際には、利用者装置2iから送信された監査要求情報及び監査情報(監査用受理証明書に加えて該監査用受理証明書の完全遅延補完データも含める)を用いて受理証明書の検証を行い、その結果を利用者装置2iに返信するイベント順序証明監査部82、及び監査用受理証明書をはじめとする監査情報を記憶する記憶部83を有する構成である。

[0104] イベント順序証明監査部82は、第1の実施の形態のイベント順序証明監査部32の機能(「ユーザ点の未来側の境界付け」)に加えて、後述する「ユーザ点の過去側の境界付け」を検証できる機能を有するようになっている。これは、あるユーザ点がある監査点よりも左にあること(即ち、時間的に前にあること)に加えて、あるユーザ点がある監査点より右にあること(即ち、時間的に後であること)を監査できることを意味する。

[0105] 以下、図14を参照しながら、この「ユーザ点の過去側の境界付け」について 説明する。

[0106] 尚、以下では、監査装置8が各順次集約期間の終了後に、その順次集約期間に取得した各監査用受理証明書の完全遅延補完データを取得することを、監査装置8は複合完全補完を行うという。

[0107] 本実施の形態においては、監査装置8は、順次集約期間が終わるごとに、該順次集約期間に受信した監査用受理証明書に対する完全遅延補完データを取得するので、監査用受理証明書に含まれる即時補完データと該遅延補完データを組み合わせることにより、監査装置8は、該順次集約期間に受信した監査用イベント受理証明書に対する完全補完データを取得することになる。

[0108] ここで、利用者装置2iと監査装置8は、第1の実施の形態で述べた条件(1)～(3)を満たすものとする。τを利用者装置2iによるユーザ点で、$T \leqq time(\tau)$を満たすものとする。$T \leqq time(\tau)$という条件から、上述の条件(1)によりτより左にある(即ち時間的に前にある)監査装置8による監査点が存在する。そのような監査点の一つを$\alpha 1$とおく。$\alpha 1$として、上記条件を満たす監査点のうち最も右に位置するものをとることにしてもよい。監査は以下の手順に従って実行される。

[0109] (1)利用者装置2iがユーザ点τで取得した受理証明書(順次集約木リーフ番号、即時補完データ)を監査装置8に送付する。

[0110] (2)監査装置8は利用者装置2iから送付された受理証明書に含まれる順次集約木リーフ番号を取り出し、該受理証明書に対応する順次集約木リーフτを特定し、自分が取得した監査用受理証明書の中から、τより左に位置する順次集約木リーフに対応するものを選ぶ。このような監査用受理証明書の中から、対応する順次集約木リーフがもっとも右に位置するものを選んでもよい。このように選ばれた監査用受理証明書に対応する順次集約木リーフを$\alpha 1$とする。

[0111] (3)監査装置8は複合完全補完を行うので、監査装置8は監査点$\alpha 1$に対応する監査用受理証明書の完全遅延補完データを取得する。該遅延補完データに対応する順次集約木リーフは、τと等しいか右に位置する(時間的に後である)。

[0112] (4)監査装置8は、監査点$\alpha 1$に対応する監査用受理証明書とそれに対する上記遅延補完データから、監査点$\alpha 1$のユーザ点τによる認証点p2の割当値を計算することができる。

[0113] (5)従って、監査装置8は、利用者装置2iから受信した順次集約木リーフ τ に対応する受理証明書内の即時補完データに、上記計算した監査点 α 1のユーザ点 τ による認証点の割当値が含まれることを検証することにより、α 1が τ より左に位置することを監査することができる。

[0114] この検証結果からまず言えることは、監査点 α 1に対応する監査装置7の監査用証明要求が証明装置7に受信された時刻をt1、 τ に対応する利用者装置2iの証明要求が証明装置7に受信された時刻をt2、この要求に対する受理証明書が証明装置7から送信された時刻をt2'とおくと、t1 < t2' ということである。

[0115] ここで、本実施の形態においても、証明装置7の直列化可能性は保証されている、即ち、t2'の時点まで証明装置7の直列化可能性は保証されているとすると、さらに、t1 < t2ということも結論できる。以上から、証明装置7がユーザ点 τ に対応する受理証明書を利用者装置2iに送信した時刻まで、証明装置7の直列化可能性が推認されるときには、監査点 α 1に対応する監査用証明要求の受付けは、ユーザ点 τ に対応する利用者装置2iの証明要求の受付けより時間的に前であることが推認される。

[0116] 尚、t2'時点までの証明装置1の直列化可能性を保証しても、利用者装置2iが受理証明の一部として即時補完データを受信していなければ、上記のことは言えないことに注意する必要がある。なぜならば、t2'時点より後で、証明装置7が監査点 α 1における割当て値を改変する可能性を除くことはできないからである。

[0117] 尚、以上の各装置は、少なくとも演算機能及び制御機能を備えた中央処理装置(CPU:Central Processing Unit)、プログラムやデータを収納する機能を有するRAM(Random Access Memory)等からなる主記憶装置(メモリ)、ハードディスク(HD)等の電源断時にもデータを記憶し続けることが出来る2次記憶装置を有する電子的な装置から構成されている。このうち、証明装置7の監査情報作成部71、並びに監査装置8の補完データ要求部81及びイベント順序証明監査部82の処理は、上記CPUによる演算制御機能を具体的に示したものに他ならない。また、証明装置7の記憶部72及び監査装置8の記憶部83は、上記主記憶装置あるいは2次記憶装置の機能を備えたものである。

[0118] また、本実施の形態に係る各種処理を実行するプログラムは、前述した主記憶装置

または2次記憶装置に格納されているものである。そして、このプログラムは、ハードディスク、フレキシブルディスク、CD－ROM、MO、DVD－ROMなどのコンピュータ読み取り可能な記録媒体に記録することも、通信ネットワークを介して配信することも可能である。

[0119] （2－2．システム動作）

次に、以上の構成を有するイベント順序証明システム200におけるイベント順序証明方法、およびイベント順序証明検証方法を図15及び図16を用いて説明する。ここで、図15は、1つの順次集約期間において証明装置7がイベント受理証明書及び監査用受理証明書を作成する動作を説明するシーケンス図であり、図16は、利用者装置2iがイベント受理証明書に対して第2の検証を行う動作を説明するシーケンス図である。

[0120] まず、図15に示すイベント順序証明方法について説明する。尚、本実施の形態に係るイベント順序証明方法において、その動作のほとんどは第1の実施の形態と同様であり、図8のステップS10～S200は、図15のステップS610～S800と同一で、その後のステップS810～S850が新たに追加されたものである。従って、以下ではこの追加されたステップについてのみ説明する。

[0121] 順次集約のための一定期間が終了すると、証明装置7の監査情報作成部71は、監査装置8からの完全遅延補完データ要求に対して、この集約期間内に発行した各監査用受理証明書の完全遅延補完データを取得し、監査装置8に送信する（ステップS810, S820, S830, S840）。

[0122] これにより、監査装置8は、各監査用受理証明書の完全遅延補完データを受信する（ステップS850）。

尚、図15に示すイベント順序証明方法においては、監査装置8の方から証明装置7に完全遅延補完データ要求を送信し、これに応えて証明装置7が監査装置8に完全遅延補完データを送信する方式であったが、これとは異なり、証明装置7が監査装置8に完全遅延補完データを自動的に送信するような方式であってもよい。

[0123] 次に、図16を参照しながら、監査装置8を用いたイベント順序証明検証方法について説明する。これは、利用者装置2iの第2の検証機能に相当するものである。ここで、

利用者装置2iの第2の検証機能に関しては、第1の実施の形態の検証機能(「ユーザ点の未来側の境界付け」)に、新たな検証機能(「ユーザ点の過去側の境界付け」)が加わったものであり、この新たな機能の動作を示すのが図16である。即ち、本実施の形態の「ユーザ点の未来側の境界付け」に関する検証処理は、第1の実施の形態で示された図10の動作と全く同一であるため、説明は省略し、「ユーザ点の過去側の境界付け」に関する検証処理について説明する。また、利用者装置2iの第1の検証機能に相当する検証方法については、第1の実施の形態における検証方法と同一であるため、説明を省略する。

[0124] まず、利用者装置2iは、監査の対象となる受理証明書(但し、即時補完データは含まれている)を含む監査要求情報を監査装置8に送信する(ステップS910, S920)。

[0125] 次に、監査装置8は送受信部31を介して監査要求情報を受信すると、イベント順序証明監査部82は、利用者装置2iから送信された監査要求情報に含まれる受理証明書が割り当てられた順次集約木のリーフ τ を特定し、該リーフ τ より左に位置する監査点 $\alpha 1$ を計算する(ステップS930, S940)。そして、この監査点 $\alpha 1$ の監査用受理証明書および該監査用受理証明書の完全遅延補完データを取得する(ステップS950)。

[0126] 続いて監査点 $\alpha 1$ のリーフ τ による認証点を計算し、監査点 $\alpha 1$ の監査用受理証明書および該監査用受理証明書の完全遅延補完データから認証点の割当値Acal を計算する(ステップS960, S970)。一方、イベント順序証明監査部82は、監査要求情報として既に受け取っている受理証明書の即時補完データからこの認証点の割当値Aを取得して、この認証点の割当値Aが、計算により求めた認証点の割当値Acalに一致するか否かを検証する(ステップS980, S990)。

[0127] 以上の検証において、検証に成功すれば、受理証明書が改ざんされていないことを確認することができる(ステップS995)。一方、検証に失敗すれば、受理証明書が改ざんされていることを確認することができる(ステップS1000)。そして、イベント順序証明監査部82は、この監査結果を送受部31を介して利用者装置2iに送信し、利用者装置2iは、監査結果を受信する(ステップS1010, S1020)。

[0128] これにより、利用者装置2iは、電子的公表機関を介した公表前においても、証明装

置7が発行した受理証明書が当該の順次集約期間において、受理証明書に含まれる元デジタル・データに対して、受理証明書に含まれる順次集約木リーフ番号で識別される順番において発行されたものであることを確実に検証することができるとともに、ユーザ点の過去側の境界付けを検証することができる。尚、上記監査結果に監査点α1の識別子を含めてもよい。この場合においては、利用者装置2iは、上記監査を要求した受理証明書に対応する証明要求の登録が、監査点α1に対応する監査用証明要求の登録より後であったことの保証を監査装置8から確実に得ることができる。

[0129] 尚、以上においては、「ユーザ点の過去側の境界付け」に関する検証処理の動作を説明したが、監査装置8は、「ユーザ点の未来側の境界付け」とともに「ユーザ点の過去側の境界付け」に関する検証処理を行うようにしてもよく、この場合には、監査要求情報として、第1の実施の形態における受理証明書および遅延補完データが必要となる。

[0130] 従って、第2の実施の形態のイベント順序証明システム200によれば、第1の実施の形態と同じ効果を得ることができる。また、これに加えて、受理証明書の正当性を検証できたときには、証明装置7において監査対象とした受理証明書の証明要求受信が監査に用いた監査用受理証明書の証明要求受信よりも時間的に後であることを証明することができる。

以上、第2の実施の形態について説明したが、第2の実施の形態には種々の変形例が考えられるものである。以下、第2の実施の形態の変形例について説明する。

[0131] (2－3. 第2の実施の形態の変形例1)

監査装置8は、上述した「ユーザ点の未来側の境界付け」及び「ユーザ点の過去側の境界付け」の機能から、2つのユーザ点の間の順序の判定を示すことも可能である。次に、2つの利用者装置2aと2bが各々、順次集約木リーフτとτ1において受理証明書を取得するとき、監査装置8がτとτ1の前後関係を監査する方法について図17を参照して説明する。ここで、図17は、監査装置8がτとτ1の前後関係を監査する動作を示すフローチャート図である。

[0132] 以下、順次集約木のリーフτ、τ1について、τ(或いはτ1)の時点とはτ(或いは

τ1)に割り付けられた順序証明要求を受信した時点を表し、τ ≦ τ1と書くことにより、τの時点以降にτ1の時点があることを表す。以下では、τとτ1の大きい方をτ2とし、τ2で受信した順序証明要求に対する受理証明の送信の時点までは証明装置1の直列化可能性が保証されているものとする。

[0133] 尚、利用者装置2a及び2bと監査装置8は、それぞれ第1の実施の形態の「ユーザ点の未来側の境界付け」の説明で述べた条件(1)～(3) を満たすものとする。

[0134] まず、監査装置8が、利用者装置2a及び2bより、各受理証明書のユーザ点間の順序判定要求を受けると、τに等しいか右に位置する監査装置8の監査点で最も左に位置するものをαとし、τ1に等しいか右に位置する監査装置8の監査点で最も左に位置するものをα1として、決定する(ステップS1110, S1120, S1130)。

[0135] 次に、監査点αとα1の時間的前後を比較する(ステップS1140)。これは、各監査点の監査用受理証明書の順次集約木番号及び順次集約木リーフ番号から判断するものである。

[0136] α < α1 のときは、第1の実施の形態の「ユーザ点の未来側の境界付け」及び上記「ユーザ点の過去側の境界付け」で述べた方法により、以下のようにτ < τ1が示される(ステップS1150)。

[0137] これは、τ1に等しいか左に位置する監査装置8の監査点でもっとも右に位置するものをα2とおくと、α ≦ α2であり、また、「ユーザ点の未来側の境界付け」で述べた方法により、τ ≦ αが示されるとともに、「ユーザ点の過去側の境界付け」で述べた方法により、α2 ≦ τ1が示されるので、以上より、τ < α ≦ α2 < τ1 となり、τ < τ1 が導かれるものである。

[0138] 同様に、α1 < α のときは、τ1 < τ が示される(ステップS1180)。

α = α1 のときは、τとτ1の前後関係の判定は、以下の手順(1)～(3)に従って行われる。

[0139] (1)利用者装置2aがτとその遅延補完点τ'で取得する情報からユーザ点τの監査点αによる認証点の位置と割当値が計算され、監査装置8が監査点αで取得する監査用受理証明書に含まれる即時補完データに上記認証点の割当値が含まれていることにより、監査装置8はτが、αより左にあること、さらにτが、αより、幾つ左にあ

るかを判定する。ここで、τが、αよりn個左にあるものとする(ステップS1160)。

[0140] (2)同様に、利用者装置2bがτ1とその遅延補完点τ1'で取得する情報からτ1の監査点αによる認証点の位置と割当値が計算され、監査装置8が監査点αで取得する監査用受理証明書に含まれる即時補完データに上記認証点の割当値が含まれていることにより、監査装置8はτ1が、αより左にあること、さらにτ1が、αより、幾つ左にあるかを判定する。ここで、τ1が、αよりn1個左にあるものとする(ステップS1160)。

[0141] (3)n > n1 のときは、監査装置8は、利用者装置2aによるユーザ点τが利用者装置2bによるユーザ点τ1より左に位置することを示すことができる(ステップS1170)。また、n < n1のときは、監査装置8は、利用者装置2aによるユーザ点τが利用者装置2bによるユーザ点τ1より右に位置することを示すことができる(ステップS1170)。

[0142] 従って、第2の実施の形態の変形例1によれば、第2の実施の形態の効果に加えて、複数の受理証明書の時間的順序の判定をすることができる。

[0143] (2－4．第2の実施の形態の変形例2)

また、監査装置8は、各順次集約期間の終了後に、その順次集約期間に取得した各監査用受理証明書の完全遅延補完データを取得する(複合完全補完を行う)と同時に、各監査用受理証明とその完全補完データから順次集約木のルート値を計算し、計算されたルート値が公表されたルート値に一致するか否かを検証することが可能である。このことを監査装置8による「複合完全化によるルート値検証」と呼ぶ。

[0144] これは、図18に示すように、監査装置8が、順次集約木のルート値を計算し、計算したルート値が、証明装置7から公表されたルート値と一致するか否かを検証することで、証明装置7による不正が行われていないことを検証するものである(ステップS1210, S1220, S1230, S1240, S1250)。

[0145] また、監査装置8は、この「複合完全化によるルート値検証」の機能により、利用者装置2iからの監査要求に含まれる監査要求情報の正当性を検証することができる。

[0146] 例えば、ある順次集約木SBTの構成終了後に、利用者装置2aが、リーフ(0, τ)の割当値を本来の割当値V(τ)から割当値v' に改変し、割当値v'がV(root(SBT))にハッシュ関数hによりリンクすることを主張したとする。このとき、第三者にこの主張を認めさせるためには、利用者装置2aは、リーフ(0, τ)の補完データ

[(v(0), LR(0)), (v(1), LR(1)), ···, (v(k-1), LR(k-1))]

を用意し、v'とこの補完データをハッシュ関数hにより所定の方式で組み合わせることによりV(root(SVT)) が計算できることを示さなければならない。この計算の過程においては、ユーザ点τの監査点αによる認証点(図11のp2)の割当値v2'も計算される。v2'はハッシュ関数の衝突困難性によって(実用上無視できる確率を除いて)round(α)において監査装置8に送付されたp2の割当値 V(p2)とは異なる。一方、監査装置8は、V(α)から出発し、authPath(α)に属するノードの割当値をハッシュ関数hによりリンクすることによりV(root(SBT))を計算する。p2はauthPath(α)に属するので、V(p2)も結合される値の1つである。ここで(実用上無視できる確率を除いて)v2' ≠ V(p2)であるから、再びハッシュ関数の衝突困難性により、利用者装置2aが計算によって示すroot(SBT)の割当値と監査装置8が複合完全化によるルート値検証において計算するroot(SBT)の割当値とは(実用上無視できる確率を除いて)異なることになる(この点についての詳細は、後述の順次集約木の性質4を参照)。従って監査装置8は利用者装置2aの主張が誤りであることを検出することができる。

[0147] 従って、第2の実施の形態の変形例2によれば、第2の実施の形態の効果に加えて、電子的情報公表機関が公表した順次集約木のルート値の正当性を検証することができる。また、監査装置8のルート値検証機能により、証明装置1及び利用者装置2iのいずれかにおいて不正があったとしても、不正の切り分けをすることができる。

[0148] (2－5. 第2の実施の形態の変形例3)

また、監査装置8は、利用者装置2iに完全補完データを提供する機能を備えることができる。以下、このことを補完データ完全化という。これは、証明装置7が障害などでサービス中断したときに有効に機能するものである。また、証明装置1がサービス中断しなくても、公表データ公開時や、補完データ要求が一時に大量に発生したときなどに証明装置7の負荷軽減に役立つものである。

[0149] 図19を参照して補完データ完全化について説明する。

[0150] 図19において、監査装置8が監査点aの完全補完データを持つならば、該完全補完データと利用者装置2iが、イベント受理証明書を取得するユーザ点uとその遅延補完データを取得する点u'で取得する情報を組み合わせることによりユーザ点uの完全

補完データを計算することができる(以下、性質P1という)。

[0151] なぜならば、図19で、j1はユーザ点uの監査点aによる認証点のレベルであり、ユーザ点uの認証パス情報のうち、レベルj1より小さいノードの情報はユーザ甲が取得しており、レベルj1以上kより小さいノードの情報は監査装置8が取得しているからである。但し、kは順次集約木の高さである。

[0152] 例えば、公開間隔が1週間とし、1日級の監査装置8(少なくとも1日に一回監査情報を取得し、各監査点の完全補完データを取得する機関)があるものとする。利用者装置2iは受理証明書を取得したのち、1日以上経過してから、遅延補完データを取得することにより、利用者装置2iの取得する情報と、監査装置8の取得する情報を組み合わせることにより利用者装置2iが取得した受理証明書の完全補完データを構成することができる(上記性質P1による)。

[0153] 次に図20を参照して、2つ以上の監査装置8i(i=a,b,n)を介して利用者装置2iが完全補完データを取得する方法について説明する。尚、監査装置8iとしては、上述した1日級の監査装置8a (少なくとも1日に一回監査情報を取得し、各監査点の完全補完データを取得する機関)と監査装置8a依存の1時間級の監査装置8b(少なくとも1時間に一回監査情報を取得し、各監査点の遅延補完データ点を監査装置8aの監査点を挟むように設定する装置)があるとする。

[0154] このとき利用者装置2iは受理証明書を所得したのち、1時間以上経過してから、遅延補完データを取得することにより、利用者装置2iの取得する情報、監査装置8bの取得する情報、及び監査装置8aの取得する情報を組み合わせることによりユーザ点の完全補完データを構成することができる。

[0155] このことは、上記性質P1を繰り返し用いることにより示される。まず、監査装置8aの取得する情報と監査装置8bの取得する情報を組み合わせることにより、監査点a2の認証パス情報が得られる。従って、図17の場合の例と同様に、ユーザ点uの認証パス情報が得られる。

[0156] 尚、上述した監査装置8a及び8bの監査点に関する条件は、例えば、監査装置8a依存の1時間級の監査装置8bは、自己の各監査点の遅延補完データを1日以上たってから取得してもよいし、あるいは1日級の監査装置8aの監査点が1日の定時(例え

ば午前0時)に取得されることが分かっていれば、毎日の監査点の遅延補完データを、その日の終了後にまとめてとるようにしてもよい。また、上記例においては2つのレベルの監査装置8iを利用しているが、同様に3つ以上のレベルの監査装置8iを利用することも可能である。

[0157] ＜第3の実施の形態＞

(3－1．システム構成)

図21は、本発明の第3の実施の形態に係るイベント順序証明システム300のシステム構成図である。イベント順序証明システム300は、イベント順序証明装置(以下、証明装置という)1、時刻情報提供装置90、複数の時刻証明利用者装置(以下、利用者装置という)10j(j=a,b, …,n)、複数のイベント順序証明利用者装置＆時刻証明装置(以下、利用者装置(時刻証明装置)という)20i(i=a,b, …,n)、イベント順序証明監査装置＆イベント時刻監査装置(以下、監査装置という)9、及び、以上の各装置を相互に接続する、例えば、インターネット網、電話回線網などにより構成されるコンピュータネットワーク4を備えており、イベント順序証明を行うとともに、時刻証明を行うコンピュータシステムとなっている。即ち、利用者装置(時刻証明装置)20iは、上記実施の形態の利用者装置2iの機能に加えて、時刻証明を行う時刻証明装置の機能も備えており、利用者装置10jからの時刻証明要求に応えて、時刻受理証明書を発行し、利用者装置10jに返信するようになっている。また、利用者装置20iが、上記時刻受理証明書のダイジェストを含むイベント順序証明要求(以下、証明要求という)を証明装置1に送信すると、証明装置1は、該証明要求に応えて、イベント順序受理証明書(以下、受理証明書という)を発行し、利用者装置20iに返信するようになっている。そして、この受理証明書に疑義が生じた場合には、利用者装置20iは、証明装置1が公表したデータ又は監査装置9による監査結果によって受理証明書を検証することができるとともに、受理証明書と時刻受理証明書が対応付けられているので、区間時刻証を取得できるようになっている。

[0158] 尚、本実施の形態においては、上記実施の形態と異なる構成及び機能を説明し、その他の構成及び機能に関しては同一部分には同一符号を付して説明を省略する。

[0159] また、上記実施の形態と同様に、第3の実施形態においても、イベント順序証明システム300のシステム構成は機能が同一であればその形態は問わないものであり、その物理的構成は種々考えられるものである。例えば、利用者装置(時刻証明装置)20iの代わりに、利用者検証装置(時刻証明装置)60iが受理証明書の検証を行うようにしてもよいし、証明装置1の代わりに、電子的情報公表装置5が証明装置1から公表データをもらい、公開するようにしてもよい。また、コンピュータネットワーク4は、郵便など他の通信手段に置き換えることも可能である。

[0160] さらに、本実施の形態においても、第1の実施の形態と同様に証明装置1の直列化可能性は保証されているものとする。保証の手段としては、第1の実施の形態におけると同様、直列化可能性監査装置を用いることにしてもよい。

[0161] 時刻情報提供装置90は、正確な時刻情報を保持して、利用者装置(時刻証明装置)20i及び監査装置9に時刻情報を提供するようになっている。

[0162] 利用者装置10jは、利用者装置(時刻証明装置)20iに所定のデジタル・データを含む時刻証明要求をし、その応答として利用者装置(時刻証明装置)20iから時刻情報が付された時刻受理証明書を取得するようになっている。

[0163] 利用者装置(時刻証明装置)20iは、上述したように利用者装置2iの機能に時刻証明装置の機能を付加した装置で、コンピュータネットワーク4を介して証明装置1、監査装置9、利用者装置10j及び時刻情報提供装置90とデータを送受信する送受信部21、利用者装置10jからの時刻証明要求を受け付けて時刻受理証明書を作成する時刻証明作成部201、時刻受理証明書ダイジェストを含む証明要求を行うイベント順序証明要求部202、現時点において取得可能な受理証明書に対する補完データを要求する補完データ要求部23、受理証明書を検証するイベント順序証明検証部204、受理証明書をはじめとするイベント順序証明に関する情報及び時刻受理証明書をはじめとする時刻証明に関する情報を記憶する記憶部205を有する構成である。尚、本実施の形態においては、イベント順序証明利用者装置として、時刻証明装置を兼ねた利用者装置を採用しているが、時刻証明装置を兼ねない利用者装置が存在してもよく、利用者装置(時刻証明装置)20iと利用者装置2iが混在するようなシステム構成としてもよい。

[0164] 詳しくは、時刻証明作成部202は、利用者装置10jから送信された所定のデジタル・データを含む時刻証明要求を受け付けて、該デジタル・データに時刻情報提供装置90から取得した時刻情報を付した時刻受理証明書を作成するようになっている。

[0165] イベント順序証明要求部203は、利用者装置10jからの時刻証明要求に対して作成された時刻受理証明書のハッシュ値である時刻受理証明書ダイジェスト(利用者装置(時刻証明装置)20iが予め用意した衝突困難一方向ハッシュ関数を時刻受理証明書に適用した結果)をイベント受理証明要求に含めるようになっている。従って、利用者装置(時刻証明装置)20iが、証明装置1から受信する受理証明書は、その構成において図6に示す通りであるが、元デジタル・データyは、上述したように、時刻受理証明書ダイジェストを含むものとなっている。

[0166] 監査装置9は、第1の実施の形態の監査装置3の機能に加えて、時刻監査装置としての機能を備えており、詳しくは、コンピュータネットワーク4を介して証明装置1、利用者装置(時刻証明装置)20i及び時刻情報提供装置90とデータを送受信する送受信部31、利用者装置20iからある受理証明書の監査要求を受けた際には、利用者装置20iから送信された監査要求情報および監査情報を用いて受理証明書の検証を行い、その監査結果を利用者装置20iに返信するイベント順序証明監査部32、及び検証した受理証明書に対応する時刻受理証明書に付された時刻の含まれる時間区間を証明する区間時刻証明証を作成する区間時刻証明証作成部91、監査用受理証明書、区間時刻証明証をはじめとする監査情報を記憶する記憶部92を有する構成である。尚、本実施の形態においては、イベント順序証明監査装置としては、イベント時刻監査装置を兼ねた監査装置を採用しているが、イベント時刻監査装置を兼ねない監査装置が存在してもよく、監査装置9と監査装置3が混在するようなシステム構成としてもよい。

[0167] 区間時刻証明証作成部91は、監査用受理証明書を証明装置1から受信したときの時刻を、時刻情報提供装置30から取得して、区間時刻証明証に付すようになっている。従って、区間時刻証明証作成部91で作成される区間時刻証明証には、本実施の形態においては、未来側の境界の時刻印が付されている。これは、第1の実施の形態で述べたように、監査装置3を用いたイベント順序証明検証(利用者装置2iの第2

の検証）により、イベント受理証明要求が割り当てられた順次集約木のリーフが監査点のリーフよりも時間的に前であることが証明できるので、イベント順序証明要求の元となる利用者装置10iからの時刻証明要求の受付が、監査装置9が監査用受理証明書を受信した時刻よりも時間的に前であることを証明するものである。ここで、本実施の形態におけるこの区間時刻証明証を「第1種の区間時刻証明証」という。

[0168] 尚、以上の各装置は、少なくとも演算機能及び制御機能を備えた中央処理装置（CPU:Centra1 Processing Unit）、プログラムやデータを収納する機能を有するRAM(Random Access Memory)等からなる主記憶装置（メモリ）、ハードディスク（HD）等の電源断時にもデータを記憶し続けることが出来る2次記憶装置を有する電子的な装置から構成されている。このうち、利用者装置（時刻証明装置）20iの時刻証明作成部202、イベント順序証明要求部203、補完データ要求部204及びイベント順序証明検証部205、並びに監査装置9の区間時刻証明証作成部91の処理は、上記CPUによる演算制御機能を具体的に示したものに他ならない。また、利用者装置（時刻証明装置）20iの記憶部206及び監査装置9の記憶部92は、上記主記憶装置あるいは2次記憶装置の機能を備えたものである。

[0169] また、本実施の形態に係る各種処理を実行するプログラムは、前述した主記憶装置または2次記憶装置に格納されているものである。そして、このプログラムは、ハードディスク、フレキシブルディスク、CD－ROM、MO、DVD－ROMなどのコンピュータ読み取り可能な記録媒体に記録することも、通信ネットワークを介して配信することも可能である。

[0170] （3－2．システム動作）

次に、以上の構成を有するイベント順序証明システム300におけるイベント順序証明方法およびイベント順序証明検証方法を図22乃至25を用いて説明する。

[0171] 尚、イベント順序証明方法においては、利用者装置（時刻証明装置）20iを利用者装置2i、監査装置9を監査装置3とすれば、全体的な動作は、図8に示す動作とほぼ同一であるため、異なる動作となる利用者装置（時刻証明装置）20iと利用者装置10j間のやりとりを中心に説明する。ここで、図20及び図23は、図8のステップS10に相当するイベント順序証明要求を送信するステップS10'を詳しく説明するシーケンス図

である(図22においては、図8のステップS60に相当する受理証明書を受信するステップS60'も含む)。また、図24は、図8のステップS120に相当する監査用受理証明書を受信するステップS120'を詳しく説明するシーケンス図である。

[0172] また、イベント順序証明検証方法の第1の検証においては、利用者装置20iを利用者装置2iとすれば、図9に示す動作と同一であるため、説明を省略する。また、イベント順序証明検証方法の第2の検証においては、監査装置9を監査装置3とすれば、図10に示す動作とほぼ同一であるため、異なる動作となる監査装置9の区間時刻証の作成について説明する。ここで、図25は、図10のステップS520に相当するイベント受理証明書の検証に成功したときのステップS520'を詳しく説明するシーケンス図である。

[0173] まず、図22を参照して、イベント順序証明方法のイベント順序証明要求を送信するステップS10'について説明する。

[0174] 利用者装置10j が利用者装置(時刻証明装置)20iにデジタル・データを含む時刻証明要求を送信すると、利用者装置(時刻証明装置)20iは送受信部201を介して、該デジタル・データを含む時刻証明要求を受信する(ステップS11'、S12')。次に、利用者装置(時刻証明装置)20の時刻証明作成部201は、時刻証明要求を受信した時刻を時刻情報提供装置90から取得し、デジタル・データに該時刻を付した時刻受理証明書を作成し、利用者装置10jに送信する(ステップS13', S14', S15')。これにより、利用者装置10jは、時刻受理証明書を受信するので、時刻受理証明書を取得することができる(ステップS16')。

[0175] 次いで、利用者装置(時刻証明装置)20iのイベント順序証明要求部203は、時刻受理証明書のダイジェストを生成し、時刻受理証明書ダイジェストを含む証明要求を作成し、証明装置1に送信する(ステップS17', S18')。この結果、証明装置1は、送受信部11を介して、証明要求を受信する(ステップS20')。

[0176] 尚、上述した方法においては、利用者装置10jに時刻受理証明書だけを返信したが、図23に示すように、利用者装置10jに時刻受理証明書に加えて、受理証明書を返信する方法も考えられる。

[0177] 図23においては、ステップS10'のイベント順序証明要求ステップでは、時刻受理証

明書を返信せずに、図8のステップS60に相当するステップS60'のイベント受理証明書受信ステップで、時刻受理証明書および受理証明書を返信する。即ち、利用者装置(時刻証明装置)20iは、証明装置1から受理証明書を受信すると、受理証明書および該受理証明書に対応する時刻受理証明書を利用者装置10jに送信するものである(ステップS61',ステップS62')。これにより、利用者装置10jは、受理証明書および時刻受理証明書の双方を受信する(ステップS63')。

[0178] 次に、図24を参照して、監査用受理証明書を受信するステップS120'について説明する。

[0179] 監査装置9は、送受信部31を介して証明装置1から監査用受理証明書を受信すると、監査用受理証明書を受信した時刻を時刻情報提供装置30から取得して、監査用受理証明書と対応付けて記憶部93に記憶する(ステップS121', S122', S123')。

[0180] 次に、図25を参照して、監査装置9によるイベント受理証明書の検証に成功したときのステップS520'について説明する。

[0181] 監査装置9のイベント順序証明監査部32が、利用者装置(時刻証明装置)20iからの監査要求に応えて受理証明書の監査を行い、監査結果がOKであるときには、さらに、監査用受理証明書に付された時刻から、第1種の区間時刻証明証を発行し、該区間時刻証明証を監査結果に含める(ステップS511', S512', S513')。

[0182] 従って、第3の実施の形態のイベント順序証明システム300によれば、第1の実施の形態と同じ効果を得ることができる。また、これに加えて、第1種の区間時刻証明証の発行により、未来側の境界の時刻印を与えることができる。

[0183] (3－3. 第3の実施の形態の変形例)

第3の実施の形態においては、第1の実施の形態の監査装置3に時刻監査装置としての機能を備えた監査装置9を用いたが、第2の実施の形態の監査装置8に時刻監査装置としての機能を備えた監査装置9'を用いて第3の実施の形態の変形例としてもよい。

[0184] この第3の実施の形態の変形例においては、区間時刻証明証作成部91'は、監査用証明要求を証明装置7に送信したときの時刻を、時刻情報提供装置30から取得して、区間時刻証明証に付すようになっている。従って、第3の実施の形態の変形例に

おいては、区間時刻証明証作成部91'で作成される区間時刻証明証には、過去側の境界の時刻印が付されている。

[0185] これは、第2の実施の形態で述べたように、監査装置8を用いたイベント順序証明検証(利用者装置2iの第2の検証)により、イベント順序証明要求が割り当てられた順次集約木のリーフがある監査点のリーフよりも時間的に後であることが証明できるので、イベント順序証明要求の元となる利用者装置10jからの時刻証明要求に対する利用者装置(時刻証明装置)20iによる時刻受理証明書の送信が、監査装置9'による監査用イベント順序証明要求の送信よりも時間的に後であることを証明するものである。ここで、この区間時刻証明証を「第2種の区間時刻証明証」という。

[0186] また、第3の実施の形態の変形例においては、監査装置9'は、「第1種の区間時刻証明証」を発行する機能も当然に有するので、未来および過去側の境界の時刻印が付された区間時刻証明証である「第3の区間時刻証明証」を発行することが可能である。これは、イベント順序証明要求の元となる利用者装置10jからの時刻証明要求の受付が、監査装置9が監査用受理証明書を受信した時刻よりも時間的に前であることを証明するとともに、イベント順序証明要求の元となる利用者装置10iからの時刻証明要求に対する利用者装置(時刻証明装置)20iによる時刻受理証明書の送信が、監査装置9'による監査用イベント順序証明要求の送信よりも時間的に後であることを証明するものである。

[0187] さらに、第3の実施の形態の変形例として、イベント順序証明システム300'は、利用者装置(時刻証明装置)20iの発行する時刻受理証明書と、該時刻受理証明書に付された時刻の時間的前、後、あるいは両方の境界を証明する1つ又は複数の区間時刻証明証を取得し、それに基づき時刻受理証明書に付された時刻の正当性を判定するイベント時刻検証装置(図19に図示せず)を有するシステム構成としてもよい。この場合においては、イベント時刻検証装置は、時刻受理証明書に付された時刻が、上記区間時刻証明証が証明する時間区間の中に、前もって定められた所定の誤差を許して含まれる割合が、前以て定められた所定の値より大きいことに基づき、時刻証明受理証明書に付された時刻の正当性を判定するようになっている。

[0188] 上記実施の形態において証明装置1及び7の電子的情報公表部17については特

に詳しく述べなかったが、好適には、電子化社会における情報公表は以下のような要件を満たすことが求められる。

[0189] (1)複数の独立なエンティティが同一の情報を公表する。

[0190] (2)上記複数のエンティティの各々に誰でもがいつでもアクセスできる。

[0191] (3)上記複数のエンティティの各々が公表する情報を取得する際に、情報提供元のエンティティ認証が提供され、かつ提供される情報の完全性が保証される。

[0192] 上記の要件のうち、要件(1)については、複数のサービス機関が、ある範囲の情報について業務として提供することにより実現できる。上記実施の形態においては、証明装置と複数の監査装置が順次集約木のルート値等について業務として情報提供を行うことにより、この要件を満足するようにしている。

[0193] 要件(2)については、現在よく普及しているWWWにより情報提供することにより実現できる。

[0194] 要件(3)については、提供する情報に対して公開鍵暗号方式に基づくデジタル署名を付することにより実現できる。この際、デジタル署名の強度が十分強いこと、及びデジタル署名に用いた署名用秘密鍵及びとそれとペアになる公開鍵のその時点での有効性が、公開鍵証明書、CRL(Certificate Revocation List)、OCSPサービス(Online Certificate Status Protocol)等を用いて公開鍵基盤(PKI: Publike-Key Infrastructure)により保証されていることが必要となる。上記の鍵ペアのは、情報の要求者が情報を取得する時点で有効であれば十分であり、随時、鍵ペアを更新し、鍵ペアの有効性を保持しつづけることが可能となる。その際、あるキー・ペアKP1 = (SK1,PK1)を新しいキー・ペアKP2 = (SK2、PK2)に置き換える際に、KP1が有効である間にKP2の署名用秘密鍵SK2によるデジタル署名を生成することは必ずしも必要ではなく、利用者がアクセスした際に、その時点で有効なキー・ペアを用いてデジタル署名を生成することが要件となる。

[0195] 従来、情報公表手段として新聞等のマスメディアに情報を公表することが行われてきたが、この方法は例えば10年後に特定のマスメディアに公表された情報にアクセスするのが容易ではないことから上記の要件(2)を満たすのが困難であること、さらにアクセスできたとしても上記の要件(3)を満たす形で情報を取得するのが困難であるこ

と等の理由で、電子化社会における情報公表の手段として必ずしも適当ではない。

[0196] ＜順次集約木の構成および性質＞

ここで、上記実施の各形態において用いられた順次集約木の動的な構成方法、および性質について説明するが、その前提としてまず、順次集約木の構成に必要な基本関数について説明する。

[0197] (基本関数)

高さkの順次集約木は、レベル0からレベルkまでのノードで構成されるが、レベルj(j＝0,1,…,k)のノードの数は、$2^{(k-j)}$であるので、レベルj、番号iのノードを(j,i)と表すことにすると、i＝0, 1,…, $2^{(k-j)}-1$となる。

[0198] 以下、実数xに対して、ceiling(x)をx以上の最小の整数、floor(x)をx以下の最大の整数として、説明する。

[0199] ノード(j, i)(但し、j ＜ k)の親は、(j＋1, floor(i/2))であるので、

parent(j, i) ＝(j＋1, floor(i/2))

と定義する。また、ノード(j, i)(但し, 0 ＜ j)の左側の子供は(j－1, 2･i)、右側の子供は(j－1, 2･i＋1)であるので、

leftChild(j, i) ＝(j－1, 2･i)

rightChild(j, i) ＝(j－1, 2･i＋1)

と定義する。このとき、高さkの順次集約木のノード(j, i)(0 ≦i＜ $2^{(k-j)}$)のルート･パスrtPathk(j, i)(ノード(j, i)からルートに至るノードの列をいう)は、

rtPathk(j,i) ＝[(j, r(j)), …, (k, r(k))]

と表すことができる。但し、r(j) ＝ I, r(j'＋1) ＝ floor(r(j')/2)(j'＜ kとし、r(j')は既に定まっているものとする)であるとする。尚、(k, r(k))は、順次集約木のルートを表し、常にr(k) ＝ 0となる。

[0200] V(j, i)はノード(j, i)の割当値である。V(0, i)をV(i)と書く。LをL ≦ kなる非負整数、SBTをある順次集約木とするとき、SBTの部分グラフBがレベルLの部分木であるとは、SBTに属するレベルLのあるノードpがあり、Bがp及びpの子孫からなるSBTの部分グラフとなっていることと定義する。

[0201] BがSBTの部分木であるとき、leafs(B)はBのリーフの集合を表すものとする。またXを

SBTのリーフからなる空でない集合とするとき，first(X)によりXのうち最も左に位置するリーフを表し、last(X)によりXのうち最も右に位置するリーフを表す。

[0202] 2つの整数i1，i2 について，[i1..i2] はi1 ≦i ≦ i2なる整数iからなる集合（区間）を表し、(i1..i2)はi1 ＜ i ≦ i2 なる整数iからなる集合（区間）を表し，[i1..i2] はi1 ≦ i ＜ i2なる整数iからなる集合（区間）を表し、(i1..i2) はi1 ＜ i ＜ i2なる整数iからなる集合（区間）を表すものとする。

[0203] （順次集約木の構成方法）

・第1の順次集約木の構成方法

上述した基本関数の定義のもと、第1の動的な集約木の構成方法について説明する。この集約木の構成方法は、深さの違いを1以内に押さえ、ダミー・ノードを作成しない方法である。

[0204] 集約期間（例えば1週間）に受付けるイベント順序証明要求の数が何らかの方法により前以て定まっているものとし、その数をnとする。このとき、集約木の高さkは，k ＝ ceiling($\log_2$(N))である。高さkの順次集約木リーフ数は最大で2^kであるので、d ＝ 2^k－nとして、レベル0のノードのうち，2d個を消去すれば、イベント順序証明要求の数nをダミー・ノードなしでリーフに割り当てることが可能となる。これは、レベル0のリーフが2d個減ると、レベル1のリーフが新たにd個できるので、合計でd個減り、リーフの数は結局、2^k－d ＝ nとなるからである。

[0205] 以下、L1W ＝ $2^{(k-1)}$（レベル1のノードの個数）、L1L ＝ $2^{(k-1)}$－d（子を有するレベル1のノードの個数）の、L0L ＝ $2(2^{(k-1)}-d)$（レベル0のノードの個数）とおくと、n個のイベント順序証明要求のうち、初めのL0L個をレベル0に配置し、残りをレベル1に配置するとき、i番目のイベント順序証明要求の配置先を表す関数place(i)は次式で表すことができる。

[0206] place(i) ＝ (0, i) (0 ≦I ＜ L0L)

place(i) ＝ (1, L1L＋i－L0L) (L0L ＜ i ≦ n)

ここで、place(i) ＝ （レベル，番号）で構成されているものである。

[0207] 図26は、第1の動的な集約木の構成方法のn ＝ 10の場合の具体例を示すものである。この場合においては、図26に示す通り、k ＝ ceiling($\log_2$(10)) ＝ 4となり、高さ

は4である。そして，d = 24－10 =6であるので、6×2＝12個のレベル0のリーフを消去する。この結果、L1W = 23 = 8, L1L = 8－6 = 2, L0L = 2×2 = 4となる。従って、レベル0のリーフが4個、レベル1のリーフが6個で，リーフの合計数はn = 10となる。この結果、図24に示すような集約木を動的に作成することができる。レベルが0より大きいノード(即ちリーフではないノード)に対する値の割当は、それが可能になったときにインクリメンタルに行われる。

[0208] ・第2の順次集約木の構成方法

次に、第2の動的な順次集約木の構成方法について説明する。この方法はインクリメンタルに集約木を構成する点では第1の方法と同じであるが、前もって定めた時間間隔(順次集約期間)に受付けるイベント順序証明要求の数は予想できないものと仮定している点が第1の方法と異なる。

[0209] ここで、インクリメンタルとは、イベント順序証明要求を受付ける都度、そこから計算できる順次集約木の部分を計算していくという意味である。以下では、受付けるイベント順序証明要求の数は予想できないが、その上界Nは見積もることができるとして説明する。この方法においては、イベント順序証明要求はすべてレベル0に割り付けられるものとし、二分木のルート値を計算するためにダミー・ノードを使用する方法である。

[0210] この方法で順次集約木を構成するとき、所定の集約期間(例えば、1週間)に受付けたイベント順序証明要求の数をNとすると、順次集約木をの高さkは、k = ceiling($\log_2$(N))である。高さkの順次集約木リーフ数は最大で2^kであるので、0からn－1までのn個のイベント順序証明要求をレベル0のノード(0, 0)からノード(0, n－1)に割り当てられることになる。

[0211] レベル0に割り当てられた、最も右のノード(0, n－1)に対して、ルート・パスrtPathk(0, n－1)が

rtPathk(j, i) = [(j, r(j)), …, (k, r(k))]

と表現されるものとする。

[0212] (一般に、rtPathk(j, i) は、rtPathk(j, i) = [(j, r(j)), …, (k, r(k))]と表現される。但し、j1 ∈ [j..k] に対して r(j1) = floor(i/$2^{(j1-j)}$)とする。)このとき、各レベルj (j＝0, …,

k－1）においては、以下のことが成り立つ。

[0213] r(j)が偶数のとき、ノード（j, r(j)＋1）はダミー・ノードとなり、$r(j)+1 < i < 2^{(k-j)}$となる各iに対して、ノード（j, i）は消去されている。

[0214] r(j)が奇数のとき、$r(j)+1 < i < 2^{(k-j)}$となる各iに対して、ノード（j, i）は消去されている。

[0215] 以上のような方法に基づいて構成される順次集約木は、ダミー・ノードは各レベルの右端でのみ現れる、および作成されるダミー・ノードの数は、k以下であるという性質を有する。

[0216] 図27及び 図28は、第2の順次集約木の構成方法のアルゴリズムを示すものであり、該アルゴリズムに従って順次集約木がインクリメンタルに構成されるようになっている。ここで、前提として以下の定義を行う。

[0217] ・$K = \mathrm{ceiling}(\log_2(N))$とする。

[0218] ・nは受付けたイベント順序証明要求の数を示す整数変数とする。初期値は0である。

[0219] ・kは定められた時間間隔が終了したときの順次集約木の高さを表す変数とする。

[0220] ・（K＋1）個のカウンタの列を，i0, …, iKとする。ここで、ijの初期値は0である（j＝0, …,K）。ijはレベルjにおいて、既に生成されたノードの数を表すと同時に、次にレベルjに作成されるノードの番号を表す。

[0221] ・（K＋1）個のブール変数の列を、b0, …, bKとする。ここで、bjの初期値はfalseである（j＝0, …,K）。bjは、レベルjにダミー・ノードがあるか否かを表す。

[0222] ・（K＋1）個の配列の列を、A0, …, AKとする。各配列は、$2^{(K-j)}$の長さをもち、レベルjのノードに割り付けられる値を保持する（j＝0, …,K）。

[0223] ・rはダミー・ノードに割り当てるダミー値を保存する変数である。

[0224] ・R(j,i)は2つの引数i,jに対してノード(j,i)に割り当てるべきダミー値を計算する関数である。

[0225] ・x, x0, x1, x2は、ノードに割り当てる値を表す変数である。

[0226] ・x1 ‖ x2は、ビット列で表された2つの値の連接である。

[0227] ・h(x) はxのハッシュ値を計算する衝突困難一方向ハッシュ関数である。

[0228] このような定義のもと、図27の処理手順1が終了すると(即ち所定の順次集約期間が終了すると)、nは受付けた時刻処理要求の数, kは生成された順次集約木の高さ, ijはレベルjのノードの数, bjはレベルjにダミー・ノードがあるか否か、Ajは, レベルjのノードに割り付けられた値からなる配列をそれぞれ表すことになる。

[0229] 図29は、第2の動的な順次集約木の構成方法のn＝9の場合の具体例を示す図である。即ち、定められた順次集約期間が終了したとき、n＝9であったとする。このとき、$k = \mathrm{ceiling}(\log_2(9)) = 4$となり、高さは4の順次集約木を構成することになる。尚、0からn－1までのn個の順序証明要求は、処理手順1により、既にノード(0,0), …, (0,n－1)に割り当てられている。また、処理手順1により、i0 ＝ 9, i1 ＝ 4, i2 ＝ 2, i3 ＝ 1, i4＝0となっている。

[0230] このとき、処理手順2の(2.2)から、ノード(0,8)のノートパスrtPath4(0,8)は

rtPath4(0,8) ＝ [(0,8), (1,4), (2,2), (3,1), (4,0)]

となる。これから、各レベルの手順は、以下の通りになる。

[0231] レベル0においては、ステップ(2.3.2.1)より、ノード(0,9)がダミー・ノードになる。レベル1においては、ステップ(2.3.3.1.5)より、ノード(1,4)に値が割り付けられ、(1,5)がダミー・ノードになる。レベル2においては、ステップ(2.3.3.1.5)より、ノード(0,2)に値が割り付けられ、(0,3)がダミー・ノードになる。レベル3においては、ステップ(2.3.3.1)により、ノード(3,1)に値が割り付けられる。レベル4においては、ステップ(2.3.3.1)により、ノード(4,0)に値が割り付けられる。

[0232] この結果、図29に示すような順次集約木をインクリメンタルに構成することができる。ダミー・ノードは各レベルに於いて高々1つである。ダミー・ノードには前以て定められた何らの手順に従いダミー・ラベル(ダミー割当値)を割当てる必要があるが、このような手順の簡単な定義としては、レベルの関数としてダミー・ラベルを定義する方法があり、これを採用してもよい。

図30は、上記のインクリメンタルな順次集約木の構成方法において各ノードに値を割付けるタイミングを示したものである。

[0233] 上述の第1及至第3の実施の形態においては、順次集約木は 図30に示すように、情報公表の区切りにおいては、ダミー・ノードを用いて最終的な順次集約木の構成

する方式を前提としている。しかし、順次集約木の具体的な構成法としてこれ以外の方法を採用することも可能である。

[0234] 即ち、上記実施の形態におけるイベント順序証明システム100、200及び300は、上述した動的な集約木の構成方法のいずれをも採用できるものであり、これにより、利用者装置からのイベント順序証明要求の量的変化に柔軟に対応することができるので、スケーラビリティの高いイベント順序証明システムを構築することが可能となる。

[0235] (認証パスの定義とそれによるルート値の計算法)

予め高さが決定しておらずインクリメンタルに構成されるような順次集約木のノードに対して、ある時点のルート・パスや認証パスを以下のように定義することができる。この定義は第1及至第3の実施の形態において所定の順次集約期間に受付ける要求の数が前以て予想できないときに適用することができる。

[0236] 現時点のリーフ番号の最大値がm(≧ 0)(従ってリーフの数がm+1)のとき、

$\kappa(m) = \min\{h | m+1 \leqq 2^h\}$ とおく。

高さが $\kappa(m)$の順次集約木を

curSBT(m)

とおく。

[0237] $p = (j, i) \in curSBT(m)$ とし、pからcurSBT(m)のルートに至るノードの並びルート・パスと言いを

rtPath(p, m)

と書く。

[0238] rtPathD(p, m)は、rtPath(p, m)に属するノードのうちでm番目のリーフの割当値が定まった時点で割当値が定まっている ノード の列である。

[0239] $rtPath(p, m) = [(0, i(0)), \cdots, (k, i(k))]$

としたとき、$0 \leqq k1 \leqq k$なるあるk1があって、

$rtPathD(p, m) = [(0, i(0)), \cdots, (k1, i(k1))]$

となることが分かる。

[0240] rtPathDV(p, m)は、rtPathD(p, m)の各ノードに割当値を割り当てたものである。

[0241] $rtPathD(p, m) = [(0, i(0)), \cdots, (k1, i(k1))]$

のとき、rtPathDV(p, m)は次のような形となる。

[0242] rtPathDV(p, m) = [((0, i(0)), v(0)), ⋯, ((k1, i(k1)), v(k1))]。

[0243] curSBT(m)における、ノード p = (j, i)からcurSBT(m)のルート値を計算するのに必要なノードp' = (j',i')の集合を該ノードの認証パスと呼びauthPathT(p, m)と表す。但し、認証パスに属する各ノードについて、該ノードを連接する方向(左又は右)についての情報もタグとして含んでいるものとする。

[0244] κ(m) = kで、

rtPath(p, m) = [(j, r(j)), ⋯, (k, r(k))]

のとき, authPathT(p, m)はrtPath(p, m)を用いて次のように表すことができる。

[0245] authPathT(p, m) =

[((j, a(j)), LR(j)), ⋯, ((k−1, a(k−1)), LR(k−1))]

ここで、r(j')が偶数の場合, a(j') = r(j')+1、r(j')が奇数の場合、a(j') = r(j')−1であり、また、r(j')が偶数の場合、LR(j') = R, r(j')が奇数の場合, LR(j') = Lである(但し、j' ∈ [j..k−1])。

[0246] そして、authPathT(p, m)の要素((j, a(j)), LR(j))について、LR(j)の部分を(LR)タグという。さらに、rtPath(p, m)の要素 (j, r(j))について、r(j)が偶数のとき、(j,r(j)+1)を(j,r(j))の右補完点といい、r(j)が奇数のとき、(j, r(j)−1)を(j, r(j))の左補完点という。

[0247] このとき、authPathT(p, m)は、rtPath(p, m)のルート以外の点の右補完点あるいは左補完点からなる。

[0248] またauthPathT(p, m)からLRタグの情報を除いたものをauthPath(p, m) と書く。即ち、

authPathT(p, m) =

[((j, a(j)), LR(j)), ⋯, ((k−1, a(k−1)), LR(k−1))]

であるとき、

authPath(p, m) = [(j, a(j)), ⋯, (k−1, a(k−1))]

とする。逆に

authPath(p, m) = [(j, a(j)), ⋯, (k−1, a(k−1))]

が与えられればauthPathT(p, m)を以下のように計算できる。j1 ∈ [j..k)に対して、rtP

ath(p, m)のレベルj1のノードは

(j1, floor(i/$2^{(j1-j)}$))

となるので、floor(i/$2^{(j1-j)}$)が偶数であるときLR(j1) = R, 奇数であるとき LR(j1) = Lと定め、

authPathT(p, m) =

[((j, a(j)), LR(j)), ⋯, ((k−1, a(k−1)), LR(k−1))]

とおけばよい。従って、authPathT(p, m)とauthPath(p, m)の一方から他方を計算することが出来る。

[0249] authPath(p, m)及びauthPathT(p, m)の中で, m番目のリーフの割当値が定まった時点で割当値が定まっているノードの集まりを各々

authPathD(p, m) 及び authPathTD(p, m)

と定義する。authPath(p, m)及びauthPathT(p, m)が上記のように表現されるとき、

k1 ≦ k−jなるkと、

j≦j(0) < j(1) < ⋯ < j(k1−1)

なる非負整数j(0), ⋯, j(k1 − 1)があり、

authPathD(p, m) = [(j(0), a(j(0))), ⋯,

(j(k1−1), a(j(k1−1)))],

authPathTD(p, m) = [((j(0), a(j(0))), LR(j(0))), ⋯,

((j(k1−1), a(j(k1−1))), LR(j(k1−1)))],

と表現される。

[0250] さらに、authPathD(p, m)及びauthPathTD(t, m)に、それに属するノードの割当値を加えたものを、各々authPathDV(p, m)及びauthPathTDV(p, m)と置く。具体的には、authPathD(p, m)及びauthPathTD(p, m)が上記のように表現されるとき、

authPathDV(p, m) =

[((j(0), a(j(0))), v(j(0)), ⋯,

((j(k1−1), a(j(k1−1))), v(j(k1−1)))],

authPathTDV(p, m) =

[((j(0), a(j(0))), LR(j(0)), v(j(0)), ⋯,

((j(k1－1), a(j(k1－1))), LR(j(k1－1)), v(j(k1－1)))]

とおく。ここで、各j' ∈ {j(0), …, j(k1−1)}に対して、v(j') = V(j', a(j')) である。

[0251] 上述の順次集約木の構成法の何れかの方法により、リーフ番号mのリーフに順次割当値を割り当てた段階で当該の順次集約木の構成が終了し、かつauthPathTDV(p, m)が上記のように表されるとき、ノードp = (j, i)の割当値V(p)とauthPathTDV(p, m)から以下のようにして集約木のルート値を計算することができる。j1 ∈ [j..k] に対して、v'(j1)を以下(1), (2)により再帰的に定義する。このとき、v'(k)が集約木のルート値となる。

[0252] (1)v'(j) = V(j, i)

(2)j1 ∈ [j..k]に対して, v'(j1)が定義されたとする、LR(j1) = Lのとき、

v'(j1+1) = h(v(j1) ‖ v'(j1))

LR(j1) = R のとき、

v'(j1+1) = h(v'(j1) ‖ v(j1))

と定義する。

[0253] m1, m2を順次集約木リーフ番号とし、m1 ≦ m2とする。このとき、

curSBT(m1) ⊆ curSBT(m2)である。

[0254] p = (j, i) ∈curSBT(m1)とする。このとき、以下の(1), (2), (3)が成立つ。

[0255] (1)rtPath(p, m1) ⊆ rtPath(p, m2)

(2)authPath(p, m1) ⊆ authPath(p, m2)

(3)authPathD(p, m1) ⊆ authPathD(p, m2)

＜順次集約木の諸性質＞

以下では、インクリメンタルに構成される順次集約木について、現時点のリーフ番号の最大値をmとし、

rtPath((0, i), m), rtPathD((0, i), m), rtPathDV((0, i), m)

を各々短く

rtPath(i, m), rtPathD(i, m), rtPathDV(i, m)

と書くこともある。同様に

authPath((0, i), m), authPathT((0, i), m), authPathD((0, i), m),

authPathTD((0, i), m), authPathDV((0, i), m), authPathTDV((0, i), m)

を各々短く

authPath(i, m), authPathT(i, m), authPathD(i, m),

authPathTD(i, m), authPathDV(i, m), authPathTDV(i, m)

と書くこともある。

[0256] 次に、順次集約木において、ユーザ点の監査点による認証点を計算するアルゴリズムについて説明する。前提として、順次集約木の高さをkとし、ユーザ点の識別番号をi0、監査点の識別番号をi1とし、i0 < i1とする。一般に、順次集約木のノード(0, i)に対してrtPath((0, i), m)は以下のように計算できる。

[0257] rtPath((0, i), m) = [(0, r(0)), ···, (k, r(k))]

但し、k = κ(m), j ∈ [0..k]に対して r(j) = floor(i/2^j)と置く。

[0258] この手順によって、ノード(0, i0)のルート・パスrtPath((0, i0), m)とノード(0, i1)のルート・パスrtPath((0, i1), m)を計算する。すると、rtPath((0, i0), m)とrtPath((0, i1), m)は、ある要素以降は一致する。このとき、最初に一致した要素を、ノード(0, i0)とノード(0, i0)の合流点(confluent point)と呼ぶ。そして，合流点のレフト・チャイルドを、ノード(0, i0)(ユーザ点)のノード(0, i1)(監査点)による認証点(authentication point)とよぶ。

[0259] 以上は、ユーザ点と監査点が同一の順次集約木に属する場合における認証点の定義であるが、該ユーザ点が属する順次集約木SBTより後に、該監査点の属す順次集約木の属する順次集約木が生成される場合には，SBTのルートを該ユーザ点の該監査点による認証点と定義する。

[0260] (順次集約木の性質1)

Bをある順次集約木の部分順次集約木で、ある時点において、last(leafs(B))に対応するラウンドの処理が終了済みとする。このとき、その時点においてBに属する各ノードの割当値は計算され割当てられている。

[0261] ・性質1の証明

図27及び図28で示されるインクリメンタルな順次集約木の構成法により、各ラウンドの終了時には、そのラウンドまでに取得できたリーフの割当値により計算できるリーフ

以外のノードの割付値は全て計算され該ノードに割当てられることになる。

[0262] last(leafs(B))に対応するラウンドの処理が終了したときには、leafs(B)に属する各リーフの割当値は定まっており、従ってBの各ノードの割当値が計算できる。従って、この段階で、Bの各ノードの割当値は計算され、各ノードに割当てられている。

予め高さが決定しておらずインクリメンタルに構成されるような順次集約木に対して、次の性質2がなりたつ。

[0263] (順次集約木の性質2)

Cを利用者装置、乙を監査装置とし、i0とi1をi0 < i1なる二つの順次集約木リーフ番号とし、round(i0)において、Cは受理証明書を受信し、乙はround(i1)において監査用受理証明書を受信したものとする。このとき、i0のi1による認証点は以下の性質を持つ。

[0264] (1)認証点の割当値は、監査点、即ちノード(0, i1)の受理証明書内補完データに含まれる。

[0265] (2)上記認証点を(j', i')とおくと、authPath((0, i0), i1)に属するノードで、レベルがj'より小さいものに対する割当値は、ノード(0, i1)に対応するラウンドで受理証明書を受理した利用者が、ノード(0, i1)に対応するラウンド以降において受信できる遅延補完データあるいは受信した受理証明書内補完データに含まれる。

[0266] 即ち、i1 ≦ i2とすると, authPath((0, i0), i1)に属するノードで、レベルがj'より小さいものに対する割当値は, EOC(i0)あるいはCToken(i0, i2)に含まれる。

[0267] (3)上記認証点の割当値及びrtPath((0, i0), i2)に属するノードでレベルが該認証点のレベルより小さいノードの割当値は、ノード(0, i0)で受理証明書を受理した利用者が、ノード(0, i1)に対応するラウンド以降において受信する遅延補完データおよびノード(0, i0)で受信した受理証明書(受理証明書内補完データを含む)から計算することができる。

[0268] ・性質2の証明

以下では、利用者に渡す受理証明書に、受理証明書内補完データ(即時補完データ)を含める場合について説明する。利用者に渡す受理証明書に受理証明書内補完データを含めず、その代わりに遅延補完データにこの情報を含める場合でも同

様の議論により同じ結論が得られる。

[0269] (1) まず、項目(1)について図31を用いつつ説明する。ここで、合流点を(j, i)、そのレフト・チャイルドである認証点を(j', i')とおく。ノード(0, i1)のcurSBT(i1)におけるルート・パスrtPath((0, i1), i1)において、(0, i1)から出発して、合流点に至る直前のノードを(j″, i″)とおく。このとき、認証点は、(j″, i″)の左補完点である。従って、認証パスauthPathT(i1, i1)の定義から、((j', i'), L)はノード(0, i1)のcurSBT(i1)における認証パスに含まれる。また, ノード(j', i')への値の割当ては, round(i1)より前に終了している。よって、((j', i'), L, V(j', i'))は(0, i1)に対する受理証明書内補完データに含まれる。

[0270] (2)次に項目(2)について図32および図33を用いつつ説明する。

[0271] $k = \kappa(i1)$ とおく。

[0272] 認証点(j', i')はノード(0, i0)のルート・パスrtPath((0, i0), i1) に含まれる。ここで、

rtPath((0, i0), i1) =

[(0,r(0)), ⋯, (j',r(j')), (j'+1,r(j'+1)), ⋯, (k,r(k))]

とする。

[0273] また、authPath((0, i0), i1)の要素で、レベルがj'より小さいノードの並びを

[(0, s(0)), ⋯, (j'−1, s(j'−1))]

とおく。

[0274] 各$j1 \in [0..j'-1]$ に対して, V(j1, r(j1))がEOC(i0)あるいはCToken(i0, i2)に含まれることを示せばよい。

[0275] authPath((0, i0), i1)の定義により、

authPath((0, i0), i1)のレベルj1の要素p2 = (j1, s(j1))は, rtPath((0, i0), i1)のレベルj1+1の要素p3 = (j1+1, r(j1+1))のライト・チャイルドであるか或いはレフト・チャイルドである。どちらであるかによって場合分けする。

[0276] (場合1)p2がp3のライト・チャイルドであるとき、図32に示すように、p2の割当値V(p2)は、$i1 \leq i2$なi2において, Cが受信できる遅延補完データ CToken(i0, i2)に含まれる。なぜならば、順次集約木の性質1により、リーフ(0, i1)に対応するラウンドのイベント順序証明処理が終わった時点で、図30のBで表されたcurSBT(i1)の部分木の割当

値は計算可能であり計算され割当て済みである。従って、その時点以降で発行される遅延補完データにはBのルートp2の割当値V(p2)が含まれる。

[0277] (場合2) p2がp3のレフト・チャイルドであるとき、図33に示すように、ノードp2の割当値V(p2)は、round(i0)のイベント順序証明要求者に対するt受理証明書内補完データに含まれる。何故ならば、図33のp2をルートとする部分木B について、

$\forall i \in leafs(B)[\, i < i0 \,]$

であり、従ってB $\subseteq$ curSBT(i0)でかつi0で識別されるラウンドの開始時に、leafs(B)の割当値は確定している。よって 順次集約木の性質1により、p2 = root(B)の割当値は、i0で識別されるラウンドにおいて確定している。従って、p2はauthPathD((0, i0), i0)に含まれる。

[0278] (3) 認証パスの定義及び項目(2)から、各j1 $\in$ [0..j']に対して、V(j1, r(j1))を以下のように再帰的に計算することが出来る。

[0279] まず、V(0, r(0))はイベント受理証明書に含まれているノード(0, i0)の割当値とする。

[0280] 次に、j1 $\in$ [0..j'−1)に対して, V(j1, r(j1))が計算されたと仮定し、V(j1+1, r(j1+1))を以下のように計算する。r(j1) < s(j1) のときは、

$V(j1+1, r(j1+1)) = h(V(j1, r(j1)) \| V(j1, s(j1)))$

とし, s(j1) < r(j1)のときは、

$V(j1+1, r(j1+1)) = h(V(j1, s(j1)) \| V(j1, r(j1)))$

とする。

[0281] 以下では、時刻の原点として、イベント順序証明システムのサービス開始時点をとり、時間を計る単位として1秒、1ミリ秒等を定め, 時刻を, 上記の原点から上記の時間の単位で計った整数で表現するものとする。また, 各監査装置 乙 は、各順次集約期間Tの最初の監査点においては、Tに閉じた監査情報に加えて、前順次集約ルート値(直前の順次集約期間T'のルート の割当値 V(root(T'))も受信するものとする。

[0282] 予め高さが決定しておらずインクリメンタルに構成されるような順次集約木に対して次の性質3がなりたつ。

[0283] (順次集約木の性質3)

以下では、Tを正整数とし、α, $\alpha 0$, τ, τ'は拡張リーフ識別子を表すものとする。

乙は監査装置とし、乙の監査点α0で、次の条件(*1)を満たすものが存在するものとする。

[0284] (*1) time(α0) ∈ [0..T)

さらに乙による任意の1つの監査点をα，その次の乙による監査点をα'とすると次の条件(*2)が成り立つものとする。

[0285] (*2) time(α')−time(α) ≦ T

また、利用者 甲 はあるイベント順序証明要求を送信し、その要求に対応する順次集約木リーフをτ，その後、該イベント受理証明書に対する遅延補完データ要求し、その要求に対応する順次集約木リーフをτ'とすると次の条件(*3)が成り立つものとする。

[0286] (*3) time(τ')−time(τ) ≧ T

さらに、監査装置 乙 は2番目以降の各順次集約期間に属する乙による最初の監査点において、直前の順次集約期間のルート値をイベント順序証明機関から受信するものとする。

[0287] このとき，以下の(1)～(4)が成り立つ。

[0288] (1) α ∈ [τ..τ'] となる乙によるある監査点αが存在する。

(2) α ∈ [τ..τ'] となる乙による監査点αについて、τのαによる認証点の割当値(ラベル)は、α以後のある順次集約木リーフ(例えばτ')において乙が受信する監査用受理証明書に含まれる。

[0289] (3)任意の順次集約木リーフτに対して、乙による監査点α'があり、次の条件(*4)が成立つ。

[0290] (*4) time(τ) ≦ time(α') < time(τ)+T

(4)T ≦ time(τ)となる任意のユーザ点τについて，α < τとなる乙の監査点αが存在する。

[0291] ・性質3の証明

(1) α ∈ [τ..τ']となるような乙によるある監査点αが存在しないと仮定する。τより左に位置する乙による監査点が存在するか否かにより場合分けする。

[0292] (場合1) τより左に位置する乙による監査点が存在する場合を考える。τより左に

位置し、τに最も近い乙による監査点をα1とし、τ'より右に位置しかつτ'に最も近い乙による監査点をα2とする。α1とα2の取り方より、

time(α1) < time(τ) 及び time(τ') < time(α2)

が成り立つ。time(α1) < time(τ) より, −time(α1) > −time(τ) となる。

[0293] 従って、

time(α2)−time(α1) > time(τ')−time(τ) ≧ T.

一方, time(α) ∈ [time(τ)..time(τ)] となるような乙によるある監査点αが存在しないのであるから、α2はα1の次の監査点である。従って上記条件(*2)より、

time(α2)−time(α1) ≦ T とならなければならない。以上から、

time(α2)−time(α1) > T かつ time(α2)−time(α1) ≦ T

となり矛盾が導かれる。従って、time(α) ∈ [time(τ)..time(τ')] となるような乙によるある監査点αが存在しないという仮定は誤りであり、time(α) ∈ [time(τ)..time(τ')] となる乙によるある監査点αが存在する。

[0294] (場合2) τより左に位置する乙による監査点が存在しない場合を考える。このとき、time(α0) ∈ [0..T]なる監査点α0について、

α0 ∈ [τ .. τ']

となることが示される。

[0295] (2) 上述の順次集約木の性質2と項目(1)から直ちに導かれる。

[0296] (3) τより前に乙の監査点が存在するか否かにより場合分けする。

[0297] (場合1) τより前に乙の監査点が存在する場合を考える。τより前で, 最も後に位置する監査点をαとし、その次の監査点の時刻をα'とする。このとき、

time(α) < time(τ) ≦ time(α')

従って、条件(*2)より、

time(α')−time(τ) < time(α')−time(α) ≦ T

よって、

time(α') < time(τ)+T

以上より、(*4)が得られる。

[0298] (場合2) τより前に乙の監査点が存在しない場合を考える。性質3の前提により、乙

の監査点α0でtime(α0) < Tとなるものがある。

[0299] time(τ) ≦ time(α0) < T

従って、

time(α0)−time(τ) < T−time(τ) ≦ T

よって、time(α0) < time(τ)+T

以上により、α' = α0として、(*4)が得られる。

[0300] (4) 乙の監査点α0で、time(α0) ∈ [0..T)となるものが存在するという上記仮定(*1)から、直ちに導かれる。

[0301] (順次集約木の性質4)

SBTを高さkの順次集約木とし、iをSBTの順次集約木リーフ番号とし、k1 ≦ kとし、authPathTk1(i)を、authPathT(i)の最初のk1個の要素の列とする。

[0302] authPathTk1(i) = [((0, i(0)), LR(0)), ⋯, ((k1−1, i(k1−1)), LR(k1−1))]

と置く。さらにここで、v1, v2を異なる2つのハッシュ値とし、AP1, AP2を次のように与える。

[0303] AP1 =

[(LR(0), v1'(0)), (LR(1), v1'(1)), ⋯, (LR(k1−1), v1'(k1−1))],

AP2 =

[(LR(0), v2'(0)), (LR(1), v2'(1)), ⋯, (LR(k1−1), v2'(k1−1))].

このとき、v1とAP1から以下の(*1)ように計算したv1''(k1)と、v2とAP2から以下の(*2)のように計算したv2''(k1)は(実用上無視できる確率を除いて)一致しない。

[0304] (*1) 各j' ∈ [0..k1] に対して、v1''(j')を以下のように再帰的に定める。

[0305] v1''(0) = v1。

[0306] j' > 0 で LR(j'−1) = L のとき、

v1''(j') = h(v1'(j'−1) ‖ v1''(j'−1))

j' > 0 で LR(j'−1) = R のとき、

v1''(j') = h(v1''(j'−1) ‖ v1'(j'−1))

(*2) 各j' ∈ [0..k]に対して、v2''(j')を以下のように再帰的に定める。

[0307] v2''(0) = v2

j' ＞ 0 で LR(j'－1) ＝ L のとき、

v2''(j') ＝ h(v2'(j'－1) || v2''(j'－1))

j' ＞ 0 で LR(j'－1) ＝ R のとき、

v2''(j') ＝ h(v2''(j'－1) || v2'(j'－1))

・性質4の証明

v1''(k1) ＝ v2''(k1)と仮定する。j' ∈ [0..k1] で v1''(j') ＝ v2''(j') となる最小のj'をj1と置く。v1 ≠ v2、即ち v1''(0) ≠ v2''(0) であるから、j1 ＞ 0 である。j0 ＝ j1－1と置く。LR(j0)がLであるか R であるかにより場合分けする。

[0308] (場合1) LR(j0) ＝ Lのとき。j1, j0のとり方より、

v1''(j0) ≠ v2''(j0)。

[0309] 従って、

v1'(j0) || v1''(j0) ≠ v2'(j0) || v2''(j0)

一方、上述の(*1), (*2) から、

v1''(j1) ＝ h(v1'(j0) || v1''(j0))

v2''(j1) ＝ h(v2'(j0) || v2''(j0))

従って、

h(v1'(j0) || v1''(j0)) ＝ h(v2'(j0) || v2''(j0))

従って、v1'(j0) || v1''(j0)とv2'(j0) || v2''(j0)が、衝突困難ハッシュ関数 hの衝突となる。

[0310] (場合2) LR(j0) ＝ R のとき、場合1に於けると同様にして、

v1''(j0) || v1'(j0)とv2''(j0) || v2'(j0)が, 衝突困難ハッシュ関数 hの衝突となることが導かれる。

[0311] 以上から、どちらの場合でも, 衝突困難ハッシュ関数 hの衝突が現れることになる。このようなことは(実用上無視できる確率を除いて)在り得ない。従って、v1''(k) ＝ v2''(k)となることも、(実用上無視できる確率を除いて)在り得ない。

[0312] 次に、上記した第1及至第3の実施の形態に係るイベント順序証明システム及びイベント順序証明監査システムを、システムを構成する各装置の資源と性能、及び装置間を結ぶネットワークの資源と性能についての種々の条件において、より実用的なも

のとした実施の形態を説明する。具体的には、木構造等の非循環有向グラフを用いて順序証明を行う場合、非循環有向グラフが計算機のメモリに収まらない場合においても実現できるようにスケーラビリティを持って実現するためには、いずれの装置(イベント順序証明装置およびそれを利用する利用者装置)も非循環有向グラフをメモリ上に展開する必要がないような方法で実現することが要求される。また同じくスケーラビリティの観点から、非循環有向グラフが大きくなっても、イベント順序証明装置とその利用者装置の間の通信量が過大とならないことが要求され、装置間の通信量が当該の非循環有向グラフのノードの数の対数のオーダで抑えられるならばこの要求は満たされる。一般に、ネットワークで結ばれた計算機システムにより所定の機能を実現するために必要なメモリ量及び装置間の通信量と、個々の装置における処理量はトレードオフの関係にあり、所定の機能を持つシステムをメモリ量、装置の処理能力、およびネットワークの伝送容量等についての種々の状況化で実用可能とするためには、処理量が実用的な範囲でメモリ量および通信量を小さくする実現方式、及び逆にメモリ量および通信量が実用的な範囲で処理量を小さくする実現方式を提供することが有用である。

[0313] ＜第4の実施の形態＞

(4－1．システム構成)

図34は、本発明の第4の実施の形態に係るイベント順序証明システム100aのシステム構成図である。イベント順序証明システム100aは、イベント順序証明装置(以下、証明装置という)1a、複数のイベント順序証明利用者装置(以下、利用者装置という)2I(I=A,B, …,N)、及び、以上の各装置を相互に接続する、例えば、インターネット網、電話回線網などにより構成されるコンピュータネットワーク3aを備えており、証明装置1aが利用者装置2Iからのイベント順序証明要求(以下、証明要求という)に応えて、イベント順序受理証明書(以下、受理証明書という)を含むイベント順序証明応答(以下、証明応答という)を利用者装置2Iに返信するようになっている。そして、利用者装置2Iは、証明装置1aから受け取ったこの複数の証明応答から受理証明書を検証することができるようになっている。

[0314] 証明装置1aは、コンピュータネットワーク3aを介して利用者装置2Iとデータの送受信

を行う送受信部11a、利用者装置2lからの証明要求として送信されたデジタル・データを順次集約木を用いてまとめるイベント順序証明要求集約部12a、受理証明書を含む証明応答を作成するイベント順序証明応答作成部13a、証明装置1が一定期間に発行した複数の受理証明書の内容を集約したデータに対して高強度デジタル署名し、公表データとするデジタル署名作成部14a、高強度デジタル署名を付加された公表データを電子的に公表する電子的情報公表部15a、及び受理証明書をはじめとするイベント順序証明に関する情報を記憶する記憶部16aを有する構成である。

[0315] 上述したように、イベント順序証明要求集約部12aは、順次集約木を用いてイベント順序証明要求をまとめるが、この順次集約木について図35を用いて説明する。図35は、一定期間（例えば1週間など証明装置1aが取り纏めデータを公表するサイクル、順次集約期間という）において、利用者装置2lからの証明要求に含まれるデジタル・データの全部あるいは一部を、所定の順次割当データ計算手順に従って計算した結果であるデジタル・データ（これを順次割当データと呼ぶ。例えば、証明要求に含まれるデジタル・データのハッシュ値）を経時的に順次左側から割り当てる値とする順次集約木の一具体例を示す図である。尚、利用者装置2lからの各証明要求が割り当てられた順次集約木のリーフを登録点ともいう。

[0316] 順次集約木の各ノード（リーフを除く）に割り当てられる値の計算方法は、以下の通りである。順次集約木の親の割当値は、左側の子の割当値H'と右側の子の割当値H"を連接（ビット列とビット列の結合）し、所定の衝突困難一方向ハッシュ関数hを適用した結果であるハッシュ値を計算することにより求められるものであり、これをh(H' ‖ H")と表す。このようにして下位のレベルの割当値から上位のレベルの割当値を計算して、最終的に最上位のレベル（ルート）の割当値（ルート値）Hを求める。

[0317] 以下においては、図35に示すように、16個のリーフを有する順次集約木の場合について説明する。尚、順次集約木リーフの数や高さは、順次集約期間が終了するまで確定しない。また、順次集約木においては、リーフへの値の割当は左から順次行われ、レベルが0より大きいノード（即ちリーフではないノード）に対する値の割当は、それが可能になったときにインクリメンタルに行われる。従って、図35の同一の縦線上にある複数のノードに対しては、値の割当が同一の処理単位の中でほぼ同時に行

われる。

ここで、順次集約木のレベルj、番号iのノードを(j,i)、(j,i)の割当値をV(j,i)と表して、図35に示す具体例を説明する。

[0318] 今、順次集約木リーフに割り当てるハッシュ値がV(0,5)であるとき(登録点が(0,5)であるとき)、このハッシュ値V(0,5)からルート値H(=V(4,0))を求めるには、V(0,5)にV(0,4)を左から連接して、ハッシュ値h1'を計算し、該ハッシュ値h1'にV(1,3)を右側から連接してハッシュ値h2'を計算し、該ハッシュ値h2'にV(2,0)を左側から連接してハッシュ値h3'を計算し、さらに該ハッシュ値h3'にV(3,1)を右側から連接してハッシュ値H(=V(4, 0))を計算すればよい。このような手順によりV(0,5)とそれを補完するデータ(ここではV(0, 4), V(1,3), V(2,0), V(3,1))からルート値Hが計算できるとき、V(0,5)はハッシュ関数hによりルート値Hにリンクするという。また、順次集約木におけるV(0,5)の補完データ(以下、順次集約補完データという)は、

[(V(0,4) , L), (V(1,3) , R), (V(2,0) , L), (V(3,1) , R)]

となる。ここで、L 及び R は、各々、2つのデジタル・データを連接する際に左から連接こと、及び右から連接することを表す。

[0319] イベント順序証明応答作成部13aは、図36に示すような受理証明書 EOC(y)を含む証明応答を作成し、利用者装置2Iに送信するようになっている。受理証明書 EOC(y)は、利用者から送付されたデジタル・データy、上述した順次割当データ計算手順によりデジタル・データyから計算された順次割当データz、順次割当データzが割当てられた順次集約木を一意に特定できる順次集約木番号、順次割当データzが割当てられた順次集約木リーフを一意に特定できる順次集約木リーフ番号、およびその時点で取得できる順次集約補完データの一部(これを登録点の即時補完データと言う)SKの位置情報及び割当値を含むように構成されている。

[0320] また、証明応答には、利用者装置2Iの過去の各登録点の遅延補完データTKの位置情報及び割当値も含むように構成されている。尚、遅延補完データTKとは、当該の証明応答発行後に取得できる順次集約補完データをいい、例えば、図35においては、V(0,5)にとって、V(2,0), V(0,4)は即時補完データであるが、V(1,3), V(3,1)はV(0, 15)が割当られた時点以降に取得可能な遅延補完データである。また、一般に、あ

るリーフa1とそれより右に位置するもう一つのリーフa2において、リーフa2の割当処理が終了した時点で定まるリーフa1の遅延補完データを、a1のa2における遅延補完データという。図35においては、ノード(0,5)のノード(0,10)における遅延補完データは、ノード(1,3)である。

[0321] ここで、本実施の形態における証明応答の具体例を図37を用いて説明する。尚、以下においては、本実施の形態における証明応答の形式を「シーケンス補完方式」と呼ぶ。今、ある利用者装置2Iからの登録点がX1(ノード(0, 2)), X2(ノード(0, 11)), X3(ノード (0, 18)), X4(ノード(0, 21)), X5(ノード(0, 29)), X6(ノード (0, 31))であるとする。

[0322] シーケンス補完の方式においては各登録点において以下のようなデータが利用者装置2Iに返されるようになっている。

[0323] (1)X1点における証明応答には、X1点の即時補完データが返される(具体的には、ノード(1,0)の割当値)。

[0324] (2)X2点における証明応答には、X2点の即時補完データ、及びX1点のX2点における遅延補完データが返される(具体的には、X2点の即時補完データとして、ノード(3,0), ノード(1,4), ノード(0,10)の割当値、X1点のX2点における遅延補完データとして、ノード(0,3), ノード(2,1))の割当値。

[0325] (3)X3点における証明応答には、X3点の即時補完データ、並びにX1点及びX2点のX3点における遅延補完データが返される(具体的には、X3点の即時補完データとして、ノード(4,0), ノード(1,8) の割当値、X1点のX3点における遅延補完データとして、ノード(0,3), ノード(2,1), ノード(3,1)の割当値、X2点のX3点における遅延補完データとして、ノード(2,3) の割当値)。

[0326] (4)X4点における証明応答には、X4点の即時補完データ、並びにX1点、X2点及びX3点のX4点における遅延補完データが返される(具体的には、X4点の即時補完データとして、ノード(4,0), ノード(2,4), ノード(0,20) の割当値、X1点のX4点における遅延補完データとして、ノード(0,3), ノード(2,1), ノード(3,1)の割当値、X2点のX4点における遅延補完データとして、ノード(2,3)の割当値、X3点のX4点における遅延補完データとして、ノード(0,19)の割当値)。

[0327] 以下、X5及びX6においても同様である。このように、シーケンス補完方式においては、証明応答として、ある登録点に関して、該登録点の即時補完データ及びある登録点より前に登録された各登録点の該登録点における遅延補完データが含まれるようになっている。尚、各証明応答は、利用者装置2lごとに管理されるようになっている。

[0328] 利用者装置2lは、コンピュータネットワーク3aを介して証明装置1aとデータを送受信する送受信部21a、所定のデジタル・データを含む証明要求を複数回行うイベント順序証明要求証部22a、証明要求に対する証明応答に含まれた受理証明書を検証するイベント順序証明検証部23a、受理証明書を含む証明応答をはじめとしてイベント順序証明に関する情報を記憶する記憶部24aを有する構成である。

[0329] ここで、イベント順序証明検証部23aは、受理証明書に対して以下の検証機能を備える。

[0330] 第1の検証機能としては、証明装置1aのデジタル署名作成部14a及び電子的情報公表部15aを介して公表される公表情報に、受理証明書に含まれる順次割当データがハッシュ関数を介してリンクすることを検証するものである。具体的には、順次集約木のルート値として公表された値と利用者装置2lで計算されたルート値が一致するか否か検証するものである。

[0331] 第2の検証機能としては、公表情報が公開される前であっても、利用者装置2lの後述する動作により、利用者装置2l間における受理証明書発行の時間的前後を検証するものである。

[0332] 以下、第2の検証機能を図38を用いて説明するが、その前に、合流点及び認証点の説明をする。

[0333] ある順次集約木のリーフaに対して、aからルートに至るパスをaのルート・パスと呼び、rtPath(a)と書く。また、rtPath(a)に属するノードのルート以外のものの兄弟ノード(sibling node)からなるノードの並びを認証パスと呼び、authPath(a)と書く。

[0334] このとき、ある順次集約木の2つのリーフa1とa2について、a1より右にa2が位置するとき、a1からルートに至るパスとa2からルートに至るパスの合流する点を、a1とa2の合流点と呼び、合流点のレフト・チャイルド(左側の子)をa1のa2による認証点と呼ぶ。例

えば、図37において、登録点X1の登録点X2による認証点は(3, 0)の点であり、登録点X2の登録点X3による認証点は(4, 0)の点である。

[0335] 今、2つの利用者装置2A及び2Bが、それぞれ、シーケンス補完方式により、各登録点の証明応答を取得するものとし、図38に示すa, a1, a2, afを利用者装置2Aの登録点、bを利用者装置2Bの登録点とする。尚、afは、暫定終端点と呼ばれるもので、利用者装置2Aの登録点のうち、最も右に位置する登録点である。図38においては、利用者装置2Aの1つの登録点aがあり、それより右に位置する利用者装置2Bの登録点bがあり、さらにその右に位置する利用者装置2Aの登録点afがある。

[0336] ここで、シーケンス補完方式においては、一般に、登録点aが登録点bより左に位置する場合、認証点のラベル(割当値)は登録点bの証明応答(即時補完データ)に含まれており、また、登録点bにおけるイベント順序証明処理が終了した時点以降(例えば、登録点afの時点)においては、登録点aの遅延補完データから計算できるラベルには、認証点のラベルが含まれるので、登録点aの登録点afにおける遅延補完データから計算される認証点の割当値と、登録点bの即時補完データに含まれる認証点の割当値が一致するか否かを検証することにより、登録点aと登録点bの時間的前後を検証することができる(詳しくは、後述の順次集約木の性質の項目(3)を参照)。

[0337] 従って、図38の場合、登録点afを現時点としたときの現時点順次集約木における、登録点aの登録点bによる認証点oの割当値V(o)が一致すれば、登録点aの登録が登録点bの登録より前に起こったことを客観的に証明することができる。イベント順序証明検証部23aは、このことを後述する動作により検証するものである。

[0338] 尚、以上の各装置は、少なくとも演算機能及び制御機能を備えた中央処理装置(CPU:Central Processing Unit)、プログラムやデータを収納する機能を有するRAM(Random Access Memory)等からなる主記憶装置(メモリ)、ハードディスク(HD)等の電源断時にもデータを記憶し続けることができる2次記憶装置を有する電子的な装置から構成されている。このうち、証明装置1aのイベント順序証明要求集約部12a、イベント順序証明応答作成部13a、デジタル署名作成部14a及び電子的情報公表部15a、並びに利用者装置2Iのイベント順序証明要求部22a及びイベント順序証明検証部23aの処理は、上記CPUによる演算制御機能を具体的に示したものに他ならない。また、

証明装置1aの記憶部16a及び利用者装置2Iの記憶部24aは、上記主記憶装置あるいは2次記憶装置の機能を備えたものである。

[0339] (4－2. システム動作)

次に、以上の構成を有するイベント順序証明システム100aにおけるイベント順序証明方法、およびイベント順序証明検証方法を図39乃至41を用いて説明する。ここで、図39は、1つの順次集約期間において証明装置1aが受理証明書を含む及び証明応答を作成する動作を説明するシーケンス図であり、図40及び41は、利用者装置2Iが受理証明書に対して第2の検証を行う動作を説明するシーケンス図である。

[0340] まず、図39を参照して、イベント順序証明方法について説明する。

[0341] 利用者装置2Iが証明装置1aにデジタル・データyを含む証明要求を送信すると、証明装置1aは送受信部11aを介して、該デジタル・データyを含む証明要求を受信する(ステップS10a, S20a)。

次に、イベント順序証明要求集約部12aが、デジタル・データyを入力の一部あるいは全部として順次割当データzを計算し、該順次割当データzを順次集約木リーフに割り当てて、インクリメンタルに順次集約木を構成していくとともに、イベント順序証明応答作成部13aは、受理証明書を含む証明応答(シーケンス補完の方式;登録点の即時補完データ及び登録点より前に登録された各登録点の該登録点における遅延補完データ)を作成し、送受信部11aを介して利用者装置2Iに証明応答を送信する(ステップS30a, S40a, S50a)。

[0342] これにより、利用者装置2Iは、受理証明書を含む証明応答を取得することができる(ステップS60a)。そして、利用者装置2Iは、このステップS10a及びS60aの証明要求送信及び証明応答受信を繰り返す。

[0343] 一方、証明装置1aでは、順次集約のための一定期間(順次集約期間)内においては、上述した証明装置1aの動作は繰り返され、順次集約期間が終了すると、電子的情報公表部17aは、順次集約木のルート値を計算し、このルート値を電子的に公表する(ステップS70a, S80a, S90a)。

[0344] 次に、図40を参照しながら、イベント順序証明検証方法について説明する。これは、利用者装置2Iの第2の検証機能に相当するものである。尚、図40は、利用者装置2

Aと2B間のデータのやりとりを示すものであるが、利用者装置2Aが利用者装置2Bに後置点判定要求(利用者装置2Aが受け取った受理証明書の登録点より時間的に後の受理証明書に対する順序判定を利用者装置2Bに要求する)行うものである。

[0345] まず、利用者装置2Aは、検証したい受理証明書EOC(a)(登録点aにおける受理証明書)を付けて後置点判定要求を利用者装置2Bに送信する(ステップS110a)。後置点判定要求を受信した利用者装置2Bは、受け取った受理証明書EOC(a)からリーフ番号n(a)を抽出し、リーフ番号n(a)より大きなリーフ番号を利用者装置2Bの登録点の中から検索する(ステップS120a, S130a)。リーフ番号n(a)より大きなリーフ番号が利用者装置2Bの登録点にある場合には、該登録点の一つbを選び、そのリーフ番号n(b)を利用者装置2Aに送信する(ステップS140a, S150a)。これに対して、リーフ番号n(a)より大きなリーフ番号が利用者装置2Bの登録点にない場合には、比較可能データなしの旨のメッセージを利用者装置2Aに送信する(ステップS142a)。

[0346] リーフ番号n(b)を利用者装置2Bから受信した利用者装置2Aは、リーフ番号n(b)より大きなリーフ番号を持つ利用者装置2Aの暫定登録点afを選び、登録点aの暫定終端点afにおける遅延補完データlateData(a,af)を取得し、利用者装置2Bに送信する(ステップS160a, S170a, S180a, S190a)。尚、比較可能データなしの旨のメッセージを利用者装置2Bから受信したときは、検証を終了する(ステップS144a)。

[0347] 利用者装置2Aから遅延補完データlateData(a,af)を受信した利用者装置2Bは、リーフ識別番号n(a)とn(b)から登録点aの登録点bに対する認証点oを計算し、受け取った受理証明書EOC(a)と遅延補完データlateData(a,af)から認証点の割当値を計算する(ステップS210a)。次に、登録点bの受理証明書EOC(b)に含まれる即時補完データに上記計算で求めた認証点の割当値が含まれているか否かを検証し、認証点の割当値が含まれているときは、登録点aが登録点bより時間的に前に登録されたという判定結果を利用者装置2Aに送信する(ステップS220a, S230a)。一方、認証点の割当値が含まれていないときは、登録点aが登録点bより時間的に前に登録されたことを証明できず、何らかの不正があるという判定結果を利用者装置2Aに送信する(ステップS220a, S240a)。

[0348] この結果、利用者装置2Aは、判定結果を受信し、取得するので、2利用者間にお

いて受理証明書発行の時間的前後を検証することができる(ステップS250a, S260a)。

[0349] 尚、上述したイベント順序証明検証方法は、利用者装置2Aが利用者装置2Bに後置点判定要求行うものであったが、前置点判定要求(利用者装置2Aが受け取った受理証明書の登録点より時間的に前の受理証明書に対する順序判定を利用者装置2Bに要求する)を行うようにしてもよい。図41は、利用者装置2Aが利用者装置2Bに前置点判定要求行う場合の利用者装置2Aと2B間のデータのやりとりを示すシーケンス図である。

[0350] まず、利用者装置2Aは、検証したい受理証明書EOC(a)(登録点aにおける受理証明書)を付けて前置点判定要求を利用者装置2Bに送信する(ステップS310a)。前置点判定要求を受信した利用者装置2Bは、受け取った受理証明書EOC(a)からリーフ番号n(a)を抽出し、リーフ番号n(a)より小さいリーフ番号、及びリーフ番号n(a)より大きいリーフ番号を利用者装置2Bの登録点の中から検索する(ステップS320a, S330a)。リーフ番号n(a)より小さいリーフ番号及びリーフ番号n(a)より大きいリーフ番号が利用者装置2Bの登録点にある場合には、リーフ番号n(a)より小さいリーフ番号の登録点bを選ぶとともに、リーフ番号n(a)より大きいリーフ番号の暫定登録点bfを選ぶ(ステップS340a, S350a)。尚、該当する登録点がない場合には、比較可能データなしの旨のメッセージを利用者装置2Aに送信する(ステップS342a)。そして、利用者装置2Aは、比較可能データなしの旨のメッセージを利用者装置2Bから受信したときは、検証を終了する(ステップS344a)。

[0351] 次いで、利用者装置2Bは、登録点bの暫定登録点bfにおける遅延補完データlateData(b,bf)を取得し、リーフ識別番号n(a)とn(b)から登録点aの登録点bに対する認証点oを計算し、受理証明書EOC(b)と遅延補完データlateData(b,bf)から認証点の割当値を計算する(ステップS360a, S370a)。次に、登録点aの受理証明書EOC(a)に含まれる即時補完データに上記計算で求めた認証点の割当値が含まれているか否かを検証し、認証点の割当値が含まれているときは、登録点aが登録点bより時間的に後に登録されたという判定結果を利用者装置2Aに送信する(ステップS380a, S390a)。一方、認証点の割当値が含まれていないときは、登録点aが登録点bより時間的に後

に登録されたことを証明できず、何らかの不正があるという判定結果を利用者装置2Aに送信する(ステップS380a, S400a)。

[0352] この結果、利用者装置2Aは、判定結果を受信し、取得するので、2利用者間において受理証明書発行の時間的前後を検証することができる(ステップS410a, S420a)。

[0353] 尚、上述したイベント順序証明検証方法は、利用者装置2A及び利用者装置2Bが受理証明書発行の時間的前後を検証したものであったが、本発明はこれに限定されず、当事者以外の第3者機関(例えば、上記第1乃至第3の実施の形態におけるイベント順序証明監査装置3)が検証を行ってもよい。この場合には、利用者装置2A及び利用者装置2Bが検証に必要な情報を第3者機関に送信し、第3者機関(イベント順序証明監査装置3)が検証を行うものである。

[0354] 従って、第4の実施の形態のイベント順序証明システム100aによれば、木構造を用いてイベント順序を証明するイベント順序証明システムにおいて、利用者装置2Iから証明要求を受付けた証明装置1aが、該証明要求に対して受理証明書を含むシーケンス補完方式(登録点に関して、該登録点の即時補完データ及び該登録点より前に登録された各登録点の該登録点における遅延補完データを証明応答に含む)による証明応答を発行し、利用者装置2Iがこの証明応答を用いて、利用者装置2I間における受理証明書発行の時間的前後を検証することができるので、証明要求をまとめた公表データが電子的に公表される前であっても、受理証明書の正当性を検証することができる。

[0355] <第5の実施の形態>

(5－1. システム構成)

図42は、本発明の第5の実施の形態に係るイベント順序証明システム200aのシステム構成図である。イベント順序証明システム200aは、証明装置4a、複数の利用者装置5I(I=A,B, …,N)、及び、以上の各装置を相互に接続する、例えば、インターネット網、電話回線網などにより構成されるコンピュータネットワーク3aを備えており、証明装置4aが利用者装置5Iからの証明要求に応えて、受理証明書を含む証明応答を利用者装置5Iに返信するようになっている。そして、利用者装置5Iは、証明装置4aから

受け取ったこの複数の証明応答から受理証明書を検証することができるようになっている。

[0356] ここで、本実施の形態と第4の実施の形態とは、証明応答の形式が異なるものであり、本実施の形態では、「シーケンス補完方式」とは別の後述する「連鎖補完方式」により証明応答が作成されるようになっている。これは、上述したシーケンス補完方式においては、各利用者装置2Iの各登録点において、当該の利用者装置2Iの過去の登録点全てに対してその遅延補完データを当該の利用者装置2Iに返送しなければならないため、過去の登録点が増加するのに比例して、証明応答のデータ量が増加するが、本実施の形態の連鎖補完方式においては、証明応答のデータ量の増加が抑制されるようになっている。尚、本実施の形態においては、上記実施の形態と異なる構成及び機能を説明し、その他の構成及び機能に関しては同一部分には同一符号を付して説明を省略する。

[0357] 証明装置4aは、コンピュータネットワーク3aを介して利用者装置5Iとデータの送受信を行う送受信部11a、利用者装置5Iからの証明要求として送信されたデジタル・データを順次集約木を用いてまとめるイベント順序証明要求集約部12a、受理証明書を含む証明応答を作成するイベント順序証明応答作成部41a、証明装置4aが一定期間に発行した複数の受理証明書の内容を集約したデータに対して高強度デジタル署名し、公表データとするデジタル署名作成部14a、高強度デジタル署名を付加された公表データを電子的に公表する電子的情報公表部15a、及び受理証明書をはじめとするイベント順序証明に関する情報を記憶する記憶部42aを有する構成である。

[0358] イベント順序証明応答作成部41aは、図43に示すような受理証明書 EOC(y)を含む証明応答を作成し、利用者装置5Iに送信するようになっている。受理証明書 EOC(y)は、利用者から送付されたデジタル・データy、上述した順次割当データ計算手順によりデジタル・データyから計算された順次割当データz、順次割当データzが割当てられた順次集約木を一意に特定できる順次集約木番号、順次割当データzが割当てられた順次集約木のリーフを一意に特定できる順次集約木リーフ番号、およびその時点で取得できる順次集約補完データの一部(これを登録点の即時補完データと言う)SKの位置情報及び割当値を含むように構成されている。

[0359] また、証明応答には、利用者装置5Iの直前の登録点の遅延補完データTK2の位置情報及び割当値も含むように構成されている。

[0360] ここで、本実施の形態における証明応答の具体例を図37を用いて説明する。尚、上述したように、この証明応答の形式を「連鎖補完方式」と呼ぶ。今、ある利用者装置5Iからの登録点がX1(ノード(0, 2)), X2(ノード(0, 11)), X3(ノード (0, 18)), X4(ノード(0, 21)), X5(ノード(0, 29)), X6(ノード (0, 31))であるとする。

[0361] 連鎖補完方式においては各登録点において以下のようなデータが利用者装置5Iに返されるようになっている。

[0362] (1)X1点における証明応答には、X1点の即時補完データが返される(具体的には、ノード(1,0)の割当値)。

[0363] (2)X2点における証明応答には、X2点の即時補完データ、及びX1点のX2点における遅延補完データが返される(具体的には、X2点の即時補完データとして、ノード(3,0), ノード(1,4), ノード(0,10)の割当値、X1点のX2点における遅延補完データとして、ノード(0,3), ノード(2,1)の割当値)。

[0364] (3)X3点における証明応答には、X3点の即時補完データ、及びX2点のX3点における遅延補完データが返される(具体的には、X3点の即時補完データとして、ノード(4,0), ノード(1,8)の割当値、X2点のX3点における遅延補完データとして、ノード(2,3)の割当値)。

[0365] (4)X4点における証明応答には、X4点の即時補完データ、及びX3点のX4点における遅延補完データが返される(具体的には、X4点の即時補完データとして、ノード(4,0), ノード(2,4), ノード(0,20)の割当値、X3点のX4点における遅延補完データとして、ノード(0,19)の割当値)。

[0366] 以下、X5及びX6においても同様である。このように、連鎖補完方式においては、証明応答として、ある登録点に関して、該登録点の即時補完データ及び該登録点の直前登録点の該登録点における遅延補完データが含まれるようになっている。これにより、連鎖補完方式においては、過去の登録点が増えても証明要求に対する証明応答のデータ量が比例的に増加しないので、証明装置4aと利用者装置5I間の通信データ量を抑制することができる。尚、各証明応答は、利用者装置5Iごとに管理されるよう

になっている。

[0367] 次に、連鎖補完方式の証明応答であっても、利用者装置5Iは、実質的には、シーケンス補完方式の証明応答と同一のデータが得られることを図44及び図45を参照して説明する。

[0368] 図44に示すように、順次集約木ST2の3つのリーフa1, a2, a3が左からこの順番であるものとすると、a2点のa3点における遅延補完データ、a2点の即時補完データ、及びa1点のa2点における遅延補完データから、a1のa3点における遅延補完データは、以下のように計算される。

[0369] まず、a2点のa3点における遅延補完データの中で最もレベルが高いノードのレベルをj2と置く。また、a1のa2による認証点をAP(a1, a2)、その兄弟ノードをAP'(a1, a2)と書き、AP(a1, a2)のレベルをj1と置く。

[0370] このとき、第1に、a1点のa3点における遅延補完データに含まれる認証パスノードのうちレベルがj1よりも小さいものの割当値は、a1点のa2点における遅延補完データに含まれる。

[0371] また、第2に、a1点のa3点における遅延補完データに含まれる認証パスノードのうちレベルがj1に等しいものの割当値は、a2点のa3点における遅延補完データおよびa2点の即時補完データから計算できる。

[0372] さらに、第3に、a1点のa3点における遅延補完データに含まれる認証パスノードのうちレベルがj1により大きいものの集合は、a2点のa3点における遅延補完データに含まれる認証パスノードのうちレベルがj1より大きいものの集合と等しい。従って、a1点のa3点における遅延補完データに含まれる認証パスノードのうちレベルがj1より大きいものの割当値は、a2点のa3点における遅延補完データから計算できる。

[0373] 以上から、a1点のa3点における遅延補完データは、以下の3つのデータから計算することができる。

[0374] (1)a2点のa3点における遅延補完データ

(2)a2点の即時補完データ

(3)a1点のa2点における遅延補完データ

尚、上記の(1)～(3)からa1点のa3点における遅延補完データを計算する処理を

完全化波及処理と呼ぶ。

[0375] この完全化波及処理を用いることにより、利用者装置5Iは、連鎖補完方式の証明応答からシーケンス補完方式の証明応答を計算することができるようになっている。図45はこの計算方法を示す表である。ここで、図45は、シーケンス補完方式及び連鎖補完方式において、各登録点に必要な即時補完データ及び遅延補完データを示している。尚、連鎖補完方式における証明応答の即時補完データ及び遅延補完データは、2重線に囲まれる部分のデータである。また、図45に示す矢印は計算の方向を示している。例えば、図45によれば、a2のa3における遅延補完データ(P1)、a2の即時補完データ(P2)、及びa1のa2における遅延補完データ(P3)から、a1のa3における遅延補完データ(P4)が計算できることを示している。

[0376] 同様にして、a3のa4における遅延補完データ(P5)、a3の即時補完データ(P6)、及びa2のa3における遅延補完データ(P1)から、a2のa4における遅延補完データ(P7)が計算できる。そして、これを繰り返すことにより、連鎖補完方式であっても、最終的には、図45に示す遅延補完データすべてが計算できることになる、これは、シーケンス補完方式の証明応答に他ならない遅延補完データである。

[0377] 従って、本実施の形態の連鎖補完方式であっても、利用者装置5Iにおいては、図45示すような完全化波及処理を行うことにより、第1の実施の形態と同様の検証をすることができるものである。尚、この完全化波及処理に関しては、後述する「インクリメンタル完全化」の処理として、詳しく説明する。

[0378] 利用者装置5Iは、コンピュータネットワーク3aを介して証明装置4aとデータを送受信する送受信部21a、所定のデジタル・データを含む証明要求を複数回行うイベント順序証明要求証部22a、証明要求に対する証明応答に含まれた受理証明書を検証するイベント順序証明検証部51a、受理証明書を含む証明応答をはじめとしてイベント順序証明に関する情報を記憶する記憶部52aを有する構成である。

[0379] ここで、イベント順序証明検証部51aは、第4の実施の形態のイベント順序証明検証部23aの機能に加えて、後述するインクリメンタル完全化の処理を行う機能を具備するもので、受理証明書に対して以下の検証機能を備える。

[0380] 第1の検証機能としては、証明装置4aのデジタル署名作成部14a及び電子的情報

公表部15aを介して公表される公表情報に、受理証明書に含まれる順次割当データがハッシュ関数を介してリンクすることを検証するものである。具体的には、順次集約木のルート値が公表された値と利用者装置5Iで計算されたルート値が一致するか否か検証するものである。

[0381] 第2の検証機能としては、公表情報が公開される前であっても、利用者装置5I間における受理証明書発行の時間的前後を検証するものである。

[0382] 以下、第2の検証機能を図39を用いて説明する。

[0383] 今、2つの利用者装置5A及び5Bが、それぞれ、連鎖補完方式により、各登録点の証明応答を取得するものとし、図39に示すa, a1, a2, afを利用者装置5Aの登録点、bを利用者装置5Bの登録点とする。尚、afは、暫定終端点である。図39においては、利用者装置5Aの1つの登録点aがあり、それより右に位置する利用者装置5Bの登録点bがあり、さらにその右に位置する利用者装置5Aの登録点afがある。

[0384] 本実施の形態においては、まず、利用者装置5Aの登録点aに対して、afを暫定終端点として、図45に示す完全化波及処理を行う。これにより、シーケンス補完方式と同一の証明応答が得られるので、その後は、第4の実施の形態のときと同一の方法を実施することにより、登録点aと登録点bの時間的前後を検証することができる。即ち、本実施の形態においても、登録点afを現時点としたときの現時点順次集約木における、登録点aの登録点bによる認証点oの割当値V(o)が一致すれば、登録点aの登録が登録点bの登録より前に起こったことを客観的に証明することができる。

[0385] 尚、以上の各装置は、少なくとも演算機能及び制御機能を備えた中央処理装置(CPU:Central Processing Unit)、プログラムやデータを収納する機能を有するRAM(Random Access Memory)等からなる主記憶装置(メモリ)、ハードディスク(HD)等の電源断時にもデータを記憶し続けることができる2次記憶装置を有する電子的な装置から構成されている。このうち、証明装置4aのイベント順序証明応答作成部41a及び利用者装置5Iのイベント順序証明検証部51aの処理は、上記CPUによる演算制御機能を具体的に示したものに他ならない。また、証明装置4aの記憶部42a及び利用者装置5Iの記憶部52aは、上記主記憶装置あるいは2次記憶装置の機能を備えたものである。

[0386] (5－2. システム動作)

ここで、以上の構成を有するイベント順序証明システム200aにおけるイベント順序証明方法に関しては、図39における証明装置1a及び利用者装置2Iを、それぞれ証明装置4a及び利用者装置5Iに置き換えたものと同一であるため、説明を省略する。また、イベント順序証明検証方法に関しては、図40及び図41における利用者装置2A及び2Bを、それぞれ利用者装置5A及び5Bに置き換えたものであるとともに、事前ステップとして、利用者装置5A及び5Bそれぞれにおいて、後述するインクリメンタル完全化処理を実行すれば、その後の動作は、図40及び図41の動作と同一であるため、説明を省略する。

[0387] ＜2－3. 証明装置4aのデータ記憶方法＞

(第1の方法)

次に、連鎖補完方式における証明装置4aのデータ記憶方法について、より詳細に説明する。まず、第1の方法は、証明装置4aが順次集約木を記憶部42a上に構成することにより、上述の連鎖補完の方式を実現する方法(以下、方法Aという)である。

[0388] 図46は、方法Aを採用したときの記憶部42aに記憶されるデータの概略構成を示す図である。図46に示すように、記憶部42aには、順次集約木そのもの、即ち、証明要求が割り当てられたノード、計算可能なノードの位置情報及び割当値を記憶するとともに、各利用者装置5Iごとに直前登録点の位置情報を記憶するようになっている。

[0389] この方法Aにおいては、証明要求を証明装置4aが受信するたびに、記憶部42a上に記憶する順次集約木に、レベルが0のノード、即ちリーフを加え、レベルが1以上のノードで割当値が計算できるものに対しては、そのノードを順次集約木に追加しその割当値を付加して、記憶部42a上に順次集約木を構築するようになっている。

[0390] 以下に、方式Aにおける証明装置4aの動作を図47を用いて説明する。ここで、図47は、証明装置4aのイベント順序証明要求集約部12a及びイベント順序証明応答作成部41aの機能を示すフローチャート図である。

[0391] まず、証明装置4aは利用者装置5Iから証明要求を受けると、証明要求から順次割当データを生成し、順次集約木の新しいリーフに割り当てて、新登録点とするとともに、該登録点のノード情報(位置情報及び割当値)を記憶する(ステップS1101a, S1103

a)。

[0392] 次いで、新登録点の即時補完データを即時補完データの定義に従って、記憶部42aに記憶された順次集約木から取得する(ステップS1105a)。

[0393] 次いで、新登録点の追加により、レベルが1以上のノードで割当値が計算できるものに対しては、割当値を計算して、そのノードの位置情報及び割当値を記憶部41aに記憶する(ステップS1107a)。

[0394] 次いで、直前登録点の遅延補完データを、遅延補完データの定義に従って、記憶部41aに記憶された利用者装置5Iごとの直前登録点及び順次集約木から取得する(ステップS1109a)。

[0395] 次いで、新登録点を直前登録点とし、該利用者装置5Iの直前登録点として記憶するとともに、ステップS1105a及びS1109aで取得した即時補完データ及び遅延補完データを含む証明応答を作成し、利用者装置5Iに送信する(ステップS1111a, S1113a, S1115a)。

[0396] (第2の方法)

次に、第2の方法は、証明装置4aが順次集約木を記憶部42a上に構成するのではなく、スタック構造を記憶部42aに構成することにより、上述の連鎖補完の方式を実現する方法(以下、方法Bという)である。方法Bは、順次集約木の大きさにほぼ比例して必要記憶量が増加する方法Aをさらに改善したものであり、スタック構造を用いて順次集約木のノード割当値、各順序証明要求に対する即時補完データ、及び遅延補完データを計算するので、必要記憶量を減少することができ、証明装置4aの記憶部42aに収まらない大きさの順次集約木の取り扱いを可能とすることができる。

[0397] 図48は、方法Bを採用したときの記憶部42aに記憶されるデータの概略構成を示す図である。図48に示すように、記憶部42aには、即時補完データ(位置情報及び割当値)を記憶する第1のスタック421aと利用者装置5Iごとに遅延補完データを記憶する記憶部422aを備えており、利用者装置5Iごとに遅延補完データを記憶する記憶部422aは、直前登録点(位置情報)423a及び遅延補完データ(位置情報及び割当値)を記憶する第2のスタック424aで構成されている。尚、第1又は第2のスタックの要素となるようなデータをスタックフレームと呼ぶ。

[0398] ここで、上記2種類のスタックのうち第1のスタックは、従来から用いられているデータ構造である。例えば、R. Merkle: Secrecy, Authentication, and Public Key Systems, UMI Research Press, 1982. の36ページには二分木のルートノードの割当て値を計算するための再帰的手順 H(a, b)が記載されているが、この再帰的手順を1つのスタックを用いて標準的に実装するとき、このスタックは上記第1のスタックと同様の使われ方をする。

[0399] 以下に、方式Bにおける証明装置4の動作を図49を用いて説明する。ここで、図49は、証明装置4aのイベント順序証明要求集約部12a及びイベント順序証明応答作成部41aの機能を示すフローチャート図である。

[0400] まず、証明装置4aは利用者装置5Iから証明要求を受けると、証明要求から順次割当データを生成し、順次集約木の新しいリーフに割り当てて、新登録点とする(ステップS1121a, S1123a)。

[0401] 次いで、新登録点の即時補完データを第1のスタック421aから取得する(ステップS1125a)。

[0402] 次いで、新登録点の位置情報及び割当値を含むスタックフレームを第1のスタックに追加する(ステップS1127a)。その際、新たに第1のスタックに追加されたスタックフレームが、他の利用者装置5Iにおいて、直前登録点の補完データに対応するものであるときは、該スタックフレームを該当する利用者装置5Iの第2のスタックに追加する(ステップS1129a, S1131a)。

[0403] 次いで、第1のスタックに兄弟ノードである2つのノードに対応する2つのスタックフレームが存在する限り、当該の2つのノードの親に当たるノードの位置情報と割当値を含むスタックフレームを生成し、当該の2つのノードに対応するスタックフレームを第1スタックから除き、上記新たに生成したスタックフレームを第1スタックに追加する(ステップS1133a, S1135a, S1137a, S1139a)。その際、新たに第1のスタックに追加されたスタックフレームが、他の利用者装置5Iにおいて、直前登録点の補完データに対応するものであるときは、該スタックフレームを該当する利用者装置5Iの第2のスタックに追加する(ステップS1141a, S1143a)。

[0404] 次いで、当該の利用者装置5Iに対する第2のスタックから直前登録点の新登録点

における遅延補完データを取得し，当該の利用者装置5Iに対する第2のスタックを空にする(ステップS1145a)。

[0405] 次いで、新登録点を直前登録点とし、該利用者装置5Iの直前登録点として記憶するとともに、ステップS1125a及びS1145aで取得した即時補完データ及び遅延補完データを含む証明応答を作成し、利用者装置5Iに送信する(ステップS1147a, S1149a, S1151a)。

[0406] 上記動作を図37に示す具体例を用いて説明する。尚、新登録点をX4として説明する。

[0407] まず、証明装置4aは利用者装置5Iから証明要求を受けると、証明要求から順次割当データを生成し、順次集約木の新しいリーフである登録点X4に割り当てて、新登録点とする(ステップS1121a, S1123a)。

[0408] 次いで、新登録点X4の即時補完データであるノード(3,0)の割当値を第1のスタック421aのスタックフレーム0から、ノード(2,4)の割当値を第1のスタック421aのスタックフレーム1から、ノード(0,20)の割当値を第1のスタック421aのスタックフレーム2からそれぞれ取得する(ステップS1125a)。

[0409] 次いで、新登録点(0,21)の位置情報及び割当値を含むスタックフレーム3を第1のスタックに追加する(ステップS1127a)。その際、新たに第1のスタックに追加されたスタックフレームが、他の利用者装置5Iにおいて、直前登録点の補完データに対応するものであるときは、該スタックフレームを該当する利用者装置5Iの第2のスタックに追加する(ステップS1129a, S1131a)。

[0410] 次いで、第1のスタックに兄弟ノードに対応する2つのスタックフレームが存在するので(スタックフレーム2及び3)、当該の2つのノードの親に当たるノード(1,10)の位置情報と割当値を含むスタックフレームを新たに生成し、当該兄弟ノードに対応するスタックフレーム(スタックフレーム2a及び3a)を第1のスタックから除き、上記新たに生成したスタックフレームを新たなスタックフレーム2aとして第1のスタックに追加する(ステップS1133a, S1135a, S1137a, S1139a)。その際、新たに第1のスタックに追加されたスタックフレームが、他の利用者装置5Iにおいて、直前登録点の補完データに対応するものであるときは、該スタックフレームを該当する利用者装置5Iの第2のスタックに追

加する(ステップS1141a, S1143a)。

[0411] 次いで、当該の利用者装置5Iに対する第2のスタックから直前登録点X3の新登録点X4における遅延補完データであるノード(0,19)の割当値を第2のスタック424aのスタックフレーム0から取得し, 当該の利用者装置5Iに対する第2のスタックを空にする(ステップS1145a)。

[0412] 次いで、新登録点X4を直前登録点X3とし、該利用者装置5Iの直前登録点423aとして記憶するとともに、ステップS1125a及びS1145aで取得した即時補完データ及び遅延補完データを含む証明応答を作成し、利用者装置5Iに送信する(ステップS1147a, S1149a, S1151a)。

[0413] (第2の方法の実装例)

以下に、上述した方法Bを用いた証明装置4aの証明応答作成の一実装例を説明する。

[0414] 図50は証明装置4aの記憶部42aの構成を示す図である。図50に示すように、順次集約木のノード割当値を計算するノード割当値計算用スタック(以下では_stackと呼ぶ)及び遅延補完用データ構造の配列(以下では_chain_comple_data_vecと呼ぶ)を持つ。_stackの要素は スタックフレームからなるスタック構造であり、各スタックフレームはplace部とvalue部からなる。このうちplace部は順次集約木のノード位置を表すプレースを保持し、そのノードのレベルを示すlevel部とレベル内の番号を示すindex部の組からなる。value部はそのノードの割当値を保持する。_chain_comple_data_vecはデータ構造chain_comple_dataの配列であり、データ構造chain_comple_dataはlate_ccomple_stack部、prev_point部、prev_point_old部、及びold_tree_id部からなる。このうち、late_ccomple_stack部は_stackと同様にスタックフレームからなるスタック構造であり、prev_point部は直前の登録点を表す識別番号(非負整数またはnil)を表し、prev_point_old部は現在の集約木より前に生成された集約木における直前の登録点を表す識別番号(非負整数またはnil)を表し、old_tree_id部はprev_point_old部がnilではないときprev_point_old部が示す登録点が属する集約木の識別番号(非負整数または nil)である。

[0415] 図51は、証明装置4aにおける連鎖補完の手順GET_REQを示す。この手順で使用

される変数及び関数は以下のとおりである。

[0416] ・v0はデジタル・データ(通常はハッシュ値)を保持する変数である。

[0417] ・idx0は利用者識別番号を表す整数を保持する変数である。

[0418] ・_lev0_ptrは次に受付けたイベント順序証明要求を割当てるリーフの識別番号を保持する変数であり、初期値は0である。

[0419] ・place0は順次集約木のノード位置を表すプレースを保持する変数である。

[0420] ・sflm0はスタックフレームを保持する変数である。

[0421] ・F(v0)はイベント順序証明要求に含まれるデジタル・データv0を順次集約木リーフに割当てるデータに変換する関数を表す。F(v0)はv0と等しいとすることにしてもよいし、あるいはv0に所定のハッシュ関数(例えば、SHA1)を適用した結果とすることにしてもよい。

[0422] ・_tree_idは順次集約木の識別番号を保持する変数である。

[0423] ・make-stackflm(place0, V0)はプレースplaceとデジタル・データV0を引数とし、place0をplace部として持ち、V0をvalue部としてもつスタックフレームを返す関数である。

[0424] ・stack_bufはある瞬間のスタックの状態を保持する変数である。

[0425] ・handle_chain_comple(id0、 tree_id0, idx0, V0,

prev_point0, immed_stack_data0, late_stack_data0)

は、順次集約木の識別子tree_id0、リーフの識別子idx0、割当てデータV0、即時補完データimmed_stack_data0、遅延補完データlate_stack_data0から構成される受理証明書を作成し、利用者識別番号id0を持つ利用者装置5iに向けて送付する関数を表す。

[0426] 証明装置4aが証明要求を受信する度に、要求者から受付けたデジタル・データをv0、要求者の識別番号をid0としてこの手順が呼び出される(ステップST101a～ST117a)。

[0427] 図52は、図51の手順GET_REQから呼び出される、ノード値計算処理の手順COMP_NODE_VALSを表す。この手順で使用される変数及び関数は以下のとおりである。

[0428] ・sflm1bはスタックフレームを保持する変数である。

[0429] ・place1bはプレースを保持する変数である。

[0430] ・idx1bは整数を保持する変数である。

[0431] ・lev1bは整数を保持する変数である。

[0432] ・val1bはデジタル・データ(通常はハッシュ値)を保持する変数である。

[0433] ・sflm0bはスタックフレームを保持する変数である。

[0434] ・place0bはプレースを保持する変数である。

[0435] ・lev0bは整数を保持する変数である。

[0436] ・lev_nw及びidx_nwは整数を保持する変数である。

[0437] ・floor(x)は実数xを引数として、xを超えない最大の整数を返す関数である。さらにy ≠ 0に対して、floor(x, y) = floor(x／y)と書く。即ち、floor(x, y)はxをyで割った際の整商である。

[0438] ・hash_comb2(val0, val1)はビット列で表される2つのデジタル・データval0とval1を引数とし、val0とval1を連接し、所定のハッシュ関数(SHA1等)を適用した結果を返す関数とする。

[0439] 図53は、図51の手順GET_REQ及び図52の手順COMP_NODE_VALSから呼び出される、遅延データ設定処理の手順REGISTER_COMPLE_DATAを表す。この手順で使用される変数及び関数は以下のとおりである。

[0440] ・placeはプレースを保持する変数であり、sflmはスタック・フレームを保持する変数である。

[0441] ・idは利用者識別番号を表す整数を保持する変数である。

[0442] ・Nは登録された利用者の総数を保持する変数である。

[0443] ・auth_node_p1(prev_point, place)は 順次リーフの識別番号である prev_pointとプレースplaceを引数とし、placeの割当値がprev_pointの遅延補完データに含めるべきものであればtrueをさもなければfalseを返す関数である。place = (j, i)としたとき、auth_node_p1(prev_point, place)がtrueとなるための必要十分条件は、floor(prev_point,2^j)が偶数で、i = floor(prev_point,2^j)+1となることである。

[0444] 次に、図54及至図56を参照しながら、1つ集約間隔が終わり、該集約間隔に対する順次集約木を終端し、次の集約間隔に対する次の順次集約木を初期化する順次集約木切替処理について説明する。

[0445] 図54は順次集約木切替処理のメインルーチンを表す。このルーチンにおいては、図55で記述されたサブルーチンTERMINATE_STREE_SUB1と図56で記述されたサブルーチンTERMINATE_STREE_SUB2を実行後、大域変数 _tree_idを1だけインクリメントし、2つの大域変数_lev0_ptrと_stackを初期化した後終了する。これらの大域変数は図51で記述した手順 GET_REQで用いたものである。

[0446] 図55で記述するTERMINATE_STREE_SUB1は、その集約間隔が終了する時点で構成されている順次集約木を基に必要に応じてノードを追加し、それらのノードには前以て定めた手順に従って所定のハッシュ値を割当、当該の集約木のルート値を定義する処理を記述している。

[0447] 図57を参照しながら、TERMINATE_STREE_SUB1の動作を、特定の状況に則して具体的に説明する。リーフ識別番号9の処理が終了後、リーフ識別番号10の処理に入る前に集約間隔が終了し、TERMINATE_STREE_SUB1を呼び出す状況を考える。開始の時点では_stackの状態は、トップから見て[(1, 4), V(1, 4)]と[(3, 0), V(3, 0)]を含むものとなっている。手順 TERMINATE_STREE_SUB1により、ノード (1,5)と(2, 3)にダミーのハッシュ値を割当て、この順次集約木のルート値を定め、同時に各登録点の完全認証パスデータ(ルート値が計算できる認証パスノードの集まり)を定義することが、以下の(1)～(4)に示すようにできる。

[0448] (1)ステップST1211aにより、局所変数sfml_xbに[(1, 4), V(1, 4)]が設定され、_stackは[(3, 0), V(3, 0)]のみを含むものとなる。次にステップST1212aにより局所変数place_xbに(1, 4)が、idx_xbに4が設定される。

[0449] ステップST1213aでは idx_xbが偶数か否かの判定をするが、現在のidx_xbの値4は偶数であるので、ステップST1214aに進む。

[0450] ステップST1214aでは_stackがnilであるか否か判定するが、_stackは nilではないのでステップST1215aに進む。

[0451] ステップST1215aでは、局所変数lev_xbに1を設定し、val_xbにV(1, 4) を設定し、idx_1bに1＋4 ＝ 5を設定する。さらに、place_1bに(lev_xb, idx_1b) ＝ (1, 5)を設定。この位置情報 (1, 5)が最初のダミー・ノードを表す。この最初のダミー・ノードに割当てるハッシュ値を計算する関数 dummy_hashを呼びだし、その返り値をdum_val_1bに設定

する。さらにsfml_1bに

make-stackflm(place_1b, dum_val_1b) = [(1, 5), dum_val_1b]

を設定する。ここでmake_stackflmはノードの位置情報とハッシュ値を引数としてスタックフレームを生成する関数である。ここでplac_1bとsfml_1b を引数としてREGISTER_COMPLE_DATA(図53で定義したもの)を呼び出す。

[0452] 続いて、ステップST1216aにおいて、lev_nwに2を設定し、idx_nwに floor(idx_xb, 2) = floor(4, 2) = 2を設定し、さらにplace_nwに(2, 2) を設定する。続いて、val_nwにhash_comb2(val_xb, dum_val_1b)を設定する。hash_comb2は2つのハッシュ値を引数として、それらを連接し、所定のハッシュ関数を適用した結果を返す関数である。sfml_nwにmake-stackflm(place_nw, val_nw)を設定し、sfml_nwを_stackにプッシュする。これにより、_stackは[(2, 2), V(2,2)], [(3, 0), V(3, 0)] を含む構成となる。更にplace_nwとsfml_nwを引数としてREGISTER_COMPLE_DATAを呼び出す。ここでステップST1211aに戻る。

[0453] (2)ステップST1211aにおいて_stackを1つポップし、sflm_xbに[(2, 2), V(2, 2)]を設定する。(ここで_stackの状態は、[(3, 0), V(3, 0)]となる。) 更にplace_xbに(2, 2)を、idx_xbに2を設定する。

[0454] ステップST1213aにおいてidx_xbの値2は偶数と判定されステップST1214aに進み、_stackはnilではないので、さらにステップST1215aに進む。lev_xbに2を設定し、val_xbにV(2, 2)を設定し、idx_1bに3を設定し、place_1bに(2, 3)を設定し、dum_val_1bにdummy_hashの返し値を設定し、この値をV(2, 3)と表す。さらにsfml_1bに

make-stackflm(place_1b, dum_val_1b) = [(2, 3), V(2, 3)]

を設定する。ここでplace_1bとsfml_1bを引数として REGISTER_COMPLE_DATAを呼び出す。

[0455] 続いて、ステップST1216aにおいて、lev_nwに3を設定し、idx_nwに floor(val_xb, 2) = floor(2, 2) = 1を設定し、さらにplace_nwに(3, 1) を設定する。続いて、val_nwにhash_comb2(val_xb, dum_val_1b)を設定し、この値をV(3, 1)と書く。sfml_nwにmake-stackflm((3, 1), V(3, 1))を設定し、sfml_nwを_stackにプッシュする。これにより、_stackは[(3, 1), V(3,1)], [(3, 0), V(3, 0)] を含む構成となる。さらにplace_nwとsfml_nwを引数として

REGISTER_COMPLE_DATAを呼び出す。ここでステップST1211aに戻る。

[0456] (3)ステップST1211aにおいて_stackを1つポップし、sflm_xbに[(3, 1), V(3, 1)] を設定する。(_stackの状態は、[(3, 0), V(3, 0)] となっている。)さらに、place_xbに(3, 1)を設定し、idx_xbに1を設定する。

[0457] ST1213aにおいてidx_xbの値1は奇数と判定され、ST1217aに進み、lev_xb に3を設定し、val_xbにV(3, 1)を設定する。_stackをポップしポップされた[(3, 0), V(3, 0)]をsfml 0bに設定する。さらに、place_0bに(3, 0)を、lev_0bに3を、idx_0bに0を、val_0bにV(3, 0)を設定する。

[0458] ステップST1218aにおいて、lev_nwに4を設定し、indx_nwにfloor(1, 2) = 0を設定し、place_nwに (4, 0)を設定し、val_nwに hash_comb2(V(3,0), V(3,1))を設定する。この値をV(4, 0)とする。 sfml_nwにmake-stackflm((4, 0), V(4, 0))を設定し、sfml_nwを_stackにプッシュする。これにより、_stackは[(4,0), V(4, 0)]を含む構成となる。 さらにplace_nwとsfml_nw を引数としてREGISTER_COMPLE_DATAを呼び出す。ここでステップST1211aに戻る。

[0459] (4)ステップST1211aにおいて、_stackを1つポップし、sflm_xbに [(4, 0), V(4, 0)]を設定する。(_stackの状態はnilとなっている。)さらに、place_xbに(4, 0)を設定し、idx_xbに0を設定する。ステップST1213aにおいてidx_xbの値0は偶数と判断され、ステップST1214aに進み_stackはnilであるので、ステップST1219aに進み、返し値にV(4, 0)を設定して終了する。

以上の結果、この手順の返し値は 当該の順次集約木のルート値である V(4,0)となる。

[0460] 次に、図56で記述されたサブルーチンTERMINATE_STREE_SUB2について説明する。

[0461] まず以下の変数および定数が使用される。

[0462] ・利用者装置の識別子である非負整数を保持する変数id

・利用者装置の総数を表す定数N

・図50の遅延補完用スタックの配列_chain_comple_data_vecの各要素と同じ構造を持つchain_comple_data2

・非負整数またはnilを保持する変数prev_chain_point2。

[0463] 次にTERMINATE_STREE_SUB2の動作について説明する。

[0464] id ＝0, …, N－1について図56のブロック1を実行する。

[0465] ブロック1の中では以下の動作をする。

[0466] chain_comple_data2に_chain_comple_data_vec[id]を設定し、prev_chain_point2にchain_comple_data2のprev_point部を設定する（ステップST1222a）。

[0467] prev_chain_point2がnilであればブロックを終了する（ステップST1223a）。

[0468] さもなければ、chain_comple_data2のprev_point_old部をprev_chain_point2に、prev_point部をnilに、old_tree部に現在の集約木識別子を各々設定し、次に_chain_comple_data_vec[id]にchain_comple_data2を設定する（ステップST1224a）。

[0469] ＜5－4．利用者装置5Iにおけるインクリメンタル完全化＞

次に、利用者装置5Iにおけるインクリメンタル完全化の処理について、詳しく説明する。ここで、インクリメンタル完全化には、大別して（1）インクリメンタル個別完全化と（2）インクリメンタル一括完全化の2つの処理があり、いずれかが利用者装置5Iにおいて実行されるものである。尚、上述した「完全化波及処理」は、インクリメンタル一括完全化の中の一機能を説明したものである。

[0470] （インクリメンタル個別完全化）

利用者装置2Aのある集約間隔Iに属するか或いは或いはその次の集約間隔の最初の登録点であるよう登録点afを暫定終端点とする。

[0471] afがある集約間隔Iの次の集約間隔の最初の登録点であるとき、当該の集約間隔Iに対する追伸点と呼ぶ。

[0472] 集約間隔Iの間に、この暫定終端点afまでに登録した登録点の集合を a(0), a(1), …, a(n)とする。（通常は、a(n) ＝ afであるが、afが追伸点であるときはこうはならない。）

このとき、登録点の集合から、afを暫定終端点としたときの1つあるいは複数の順次集約小木が構成され、構成された順次集約小木の集まりを、afを暫定終端点としたときの順次集約フォレストと呼ぶことにする。

[0473] 図58を参照して、順次集約フォレストと順次集約小木について具体的に説明する。

[0474] afが当該の集約間隔にあるとき、afがリーフ番号（非負整数）を表し、afの二進表現

においてはk(1), k(2), …,k(m)桁において1が立つものとする(但し最小桁は0桁とする)。図58においては、m = 4としている。ここで、k(m)は0でもよく、k(1) > k(2) > k(3) > … > k(m)とならなければならない。このとき、上記順次集約フォレストに属するn番目の順次集約小木のリーフの数は$2^{k(n)}$となる。図58においては、ST2(1), …, ST2(4)が順次集約小木を表している。

[0475] インクリメンタル個別完全化とは、指定されたa ∈ {a(0), a(1), …, a(n)}について、以下の計算(1)～(3)を行うことである。

[0476] (1)aが属する順次集約小木ST(ユニークに定まる)を計算する。

[0477] (2)順次集約フォレストにおいて上記STより左に位置する1つあるいは複数の順次集約小木のルートの割当値を、a(0), …, a(n)(及びaf)で取得する補完データから計算する。

[0478] (3)STにおけるaの認証パスをauthPathST(a)とおくと、authPathST(a) に属するノードの割当値を、a(0), …, a(n)(及びaf)で取得する補完データから計算する。

[0479] 尚、インクリメンタル個別完全化の定義は、以下に定義する現時点順次集約木を用いて行うこともできる。ここで、現時点順次集約木とは、afを暫定終端点としたときの順次集約フォレストを含むような最小の二分木を、afを暫定終端点としたときの現時点順次集約木という。

[0480] 図59は、現時点順次集約木の枝を実線及び点線で示すものである。このうち、点線で示す枝が順次集約フォレストには含まれないが現時点順次集約木を構成するために追加した枝である。また黒で塗りつぶされた小円が順次集約フォレストに含まれるノードであり、塗りつぶしがない小円が現時点順次集約木を構成するために追加したノードである。現時点順次集約木をCSTと表し、CSTにおけるaの認証パスを authPathCST(a)とおく。このとき、インクリメンタル個別完全化とは、指定されたa ∈ {a(0), a(1), …, a(n)} について、authPathCST(a)に属し、既に割当値が定まっているノードの割当値を、a(0), …, a(n)(及びaf)で取得する補完データから計算することと同値である。

[0481] 尚、順次集約フォレストのリーフの数の総数をNとしたとき、現時点順次集約木の高さhは$N \leq 2^k$となる最小の非負整数kとなる。

[0482] 上述したことを踏まえて、第2の検証機能を説明した図38に戻ると、登録点aに対して、afを暫定終端点としてインクリメンタル個別完全化を行うと、認証点oの割当値V(o)が計算できることになる。これにより、登録点afを現時点としたときの現時点順次集約木における、登録点aの登録点bによる認証点oの計算された割当値V(o)が、登録点bで取得される即時補完データに含まれれば、登録点aの登録が登録点bの登録より前に起こったことを客観的に証明することができる。

[0483] 次に、図60及び図61を参照しながら、インクリメンタル完全個別化の動作について説明する。図60は、インクリメンタル完全個別化の動作を示すフローチャート図である。

[0484] まず、暫定終端点afより以前の登録点で集約間隔lに属する登録点aを1つ指示する(ステップS510a)。図61に示す順次集約フォレストにおいては、インデックス18のリーフ(ノード(0,18))をaとしている。

[0485] 次に、登録点aが属する順次集約小木STを計算する(ステップS520a)。図61に示す順次集約フォレストにおいては、構成済み順次集約小木のうち左から2番目のST2(2)がSTとなる。

[0486] 次に、登録点aのSTにおける各遅延認証パスノードsを計算する(ステップS530a)。図61に示す順次集約フォレストにおいては、インデックス19のリーフ(ノード(0,19))とレベル2のインデックス5のノード((ノード(2,5))が遅延認証パスノードとなる。

[0487] 次に、各遅延認証パスノードsの取得参照点をそれぞれ決定する(ステップS540a)。ここで、取得参照点及び取得タイミング点について説明する。尚、以下では、ある登録点aの即時補完データと、aの次の登録点a1で取得されるaの遅延補完データの合併を、登録点aの連鎖補完データとよぶ。

[0488] 登録点a0が与えられたとき、そのauthPath(a0)でレベルjのノード(j, s(j))の割当値V(j, s(j))を計算するために十分な情報を補完データから直接取得できるかあるいは該データを基に計算により取得できる要求登録点をV(j, s(j))の取得参照点と呼ぶ。そして、上記の必要な補完データを受信する登録点を取得タイミング点と呼ぶ。

[0489] 例えば、図37に示す順次集約木において、登録点X3が与えられたとき、遅延補完データの1つであるノード(0,19)の取得参照点は、登録点X3(ノード(0,18))、取得タ

イミング点は、登録点X4(ノード(0,21))となる。また、登録点X3が与えられたとき、即時補完データの1つであるノード(4,0)の取得参照点及び取得タイミング点は、登録点X3(ノード(0,18))となる。一般に、即時補完データに関しては、取得参照点と取得タイミング点は一致する。

[0490] 次に、ステップS540aで決定された取得参照点をもとに、各認証パスノードsの割当値を計算する(ステップS550a)。

[0491] 以上により、登録点aにおけるインクリメンタル完全化の処理が終了し、この計算結果を用いて、登録点aの割当値を含む入力に衝突困難ハッシュ関数を適用し、V(root(ST))を計算することができる。尚、上述した計算が可能であるのは、sの割当値の取得参照点および取得タイミング点がともに、暫定登録点af以前であることによる。

[0492] (インクリメンタル個別完全化の実装例)

以下に、上述したインクリメンタル個別完全化の一実装例を説明する。

[0493] まず、順次集約小木STを決定する計算手順FOREST_SSTを図62に示す。これは、図62のステップS520aに相当するものである。

[0494] この手順で使用される変数及び関数は以下のとおりである。

[0495] ・入力としては、リーフ識別子a(非負整数)、暫定終端点の識別子fin(非負整数)

・出力としては、aが属する順次集約小木の一番左のリーフ識別子start(非負整数)、aが属する順次集約小木の一番左のリーフ識別子last(非負整数)

・変数としては、非負整数を保持する変数rest, ht, leaf_num

・使用される関数として、$\log_2(x)$は、$\log_2(x)$以下の最大の整数、expt(x, y)は、xのy乗

このアルゴリズムは、リーフ識別子a(非負整数)と暫定終端点の識別子 fin (非負整数)を入力とし、該暫定終端点の登録が終了した時点における順次集約フォレストに属する順次集約小木でaが属するものをSTとしたとき、STの一番左に位置するリーフの識別子start(非負整数)と一番右に位置するリーフの識別子last(非負整数)の組を出力するものである。当該の順次集約小木STのリーフの数は、last－start＋1となり、当該の順次集約小木の高さは、$\log_2(\text{last}-\text{start}+1)$となる。

[0496] 図61で示した具体例について、図62の手順を適用すると以下のようになる。リーフ識別子aを18とおき，暫定終端点の識別子finを26とおく。このとき、図62の手順に従

って計算すると、startとして16が返され、lastとして23が返される。この出力から、aが属する順次集約小木は、図61のST2(2)であることが分かる。

[0497] 次に、インクリメンタル完全化における認証パスノード割当値の取得参照点決定手順DECIDE_GET_POINT_Aを図63に示す。この手順は、指定された要求登録点の指定されたレベルの認証パスノードの割当値が、どの要求登録点の即時補完データあるいは遅延補完データから得られるかを決定するものであり、図60のステップS540aに相当するものである。

[0498] 図64は、手順DECIDE_GET_POINT_Aにおいて使われるデータ構造と変数の一部を表す。データ構造chaindataはleaf_index部、rgt_value部、immediate部、late部からなる構造である。Mを一つの利用者装置5Iが一つの集約間隔に送出する順序証明要求の最大数とする。

[0499] この手順で使用されるその他の変数及び関数は以下のとおりである。

[0500] ・変数chiandata_storeは要素数がMの配列で、配列の各要素がデータ構造chaindataを保持するようなものである(図64参照)。

[0501] ・chaindata0はデータ構造chaindataを保持する変数である。

[0502] ・a0は順次集約木のリーフ識別子を表す整数を保持する変数である。

[0503] ・順次集約木のノード(j,i)に対して、subTree(j, i)は(j, i)をルートとするような順次集約木の部分木を表す。

[0504] ・順次集約木の部分木STに対して、leafs(ST)はSTのリーフの集合を表す。例えば、leafs(subTree(j, i))は部分木subTree(j, i)のリーフの集合である。また、height(ST)はSTの高さを表す。

[0505] 次に、図63に示すインクリメンタル完全化の認証パスノード割当値の取得参照点決定手順(DECIDE_GET_POINT_A)のアルゴリズムの根拠を図65に示す図をもとに説明する。

[0506] ここで、afを暫定終端点とする構成済みフォレスト内の順次集約小木のうちa0が属すものをSTとおく(a0 ∈ leafs(ST))。

[0507] また、ST内のa0の認証パスをauthPathST(a0)とおき、

$$authPathST(a0) = [(0, s(0)), (1, s(1)), \cdots, (k-1, s(k-1))]$$

と置く。(但し、kは構成済みフォレスト内のaが属する順次集約小木STの高さである。即ち、k = height(ST)。)以下では、非負整数n, mに対して、[n…m]はn以上でm以下の整数の集合を表すものとする。

[0508] 各j ∈ [0… k－1]に対して、(j, s(j))がどの登録点の補完データから計算できるかを決定するアルゴリズムを以下に示す。

[0509] rtPathST(a0)をSTにおけるaのルート・パスとおき、

rtPathST(a0) = [(0, r(0)), (1, r(1)), …, (k－1, r(k－1)), (k, r(k))]

とする。r(0) = a0 、root(ST) = (k, r(k)) である。j ∈ [0…k－1]とする。

[0510] (1)(j, r(j))が(j+1, r(j+1))のleft-childであるとき

s(j) = r(j)+1 であり、(j, s(j))は(j+1, r(j+1))のright-childである。leafs(subTree(j, r(j)))に属する要求登録点の中で、最も右に位置する点を計算し、a1と置く。

[0511] (1－1)a1 ≠ afのとき

a1の次の要求登録点をa2と置く(a1 ≠ afではないのでこのようなa2が在る。a2 ≦ af)。

[0512] (1－1－1)a2 ∈ leafs(subTree(j, s(j)))のとき

leafs(subTree(j, s(j)))に属する要求登録点で最も右に位置するものをa3 と置く。

[0513] (1－1－1－1)a3 = last(leafs(subTree(j, s(j)))であるとき(図65(a)を参照)

即時補完データimmedData(a3)は、subTree(j, s(j))におけるa3の完全補完データcmpltData(subTree(j, s(j)), a3)を含む。従って、

immedData(a3) ⊢ V(j, s(j))

(尚、X ⊢ Yは, X からYが計算できることを表す。)

このとき、V(j, s(j))の取得参照点および取得タイミング点は共にa3としてよい。

[0514] (1－1－1－2)a3 ≠ last(leafs(subTree(j, s(j)))であるとき

(1－1－1－2－1)a3 ≠ afであるとき(図65(b)を参照)

a3の次の要求登録点をa4と置く。(a3 ≠ afなので、このようなa4がある。a4 ≦ af。a4は追伸点である可能性もある。)

a3のa4による認証点のレベルをj'とすると、j' ≧ j+1

従って、順次集約木の性質により、V(j, s(j))はa3で取得する即時補完データと、a4で

取得する(a3に対する)遅延補完データから計算できる。即ち、

immedData(a3)∪lateData(a3,a4) ⊢ V(j, s(j))

(尚、aをa3のa4による認証点とすると、immedData(a4)にはV(a)が入っているが、これがV(j, s(j)) とは限らないことに注意する必要がある。)

このとき、V(j, s(j))の取得参照点をa3、取得タイミング点をa4としてよい。a3 ≦ afかつa4 ≦ afである。

[0515] (1－1－1－2－2)a3 ＝ afであるとき(図65(c)を参照)

このとき、afを暫定終端点とする構成済みフォレストにおいて(j, s(j)) を含む順次集約小木はない。

[0516] よって, STは(j, s(j))を含むことは無い。従ってこのような場合はあり得ない。

[0517] (1－1－2)a2 ∈ leafs(subTree(j, s(j)))ではないとき(図65(d)を参照)

V(j, s(j)) ∈ lateData(a1, a2)である。

[0518] V(j, s(j))の取得参照点をa1、V(j, s(j))の取得タイミング点をa2としてよい。

[0519] a1 ≦ afかつa2 ≦ af

(1－2)a1 ＝ afであるとき(図65(e)を参照)。

[0520] このとき、afを暫定終端点とする構成済みフォレスト内に(j, s(j))を含む順次集約小木はない。

[0521] よって、STは(j, s(j))を含むことは無い。従って、このような場合はあり得ない。

[0522] (2)(j, r(j))が(j+1, r(j+1))のright-childであるとき(図65(f)を参照)

r(j) ＝ s(j)+1であり、(j, s(j))は(j+1, r(j+1))のleft-childである。

[0523] V(j, s(j)) ∈ immedData(a)

V(j, s(j))の取得参照点および取得タイミング点を共にa0としてよい。a0≦ af

以上から、図63に示すインクリメンタル完全化の認証パスノード割当値の取得参照点決定手順(DECIDE_GET_POINT_A)は、すべての場合分けを考慮した手順となっているので、図63に示すアルゴリズムは正しいことがわかる。

[0524] 次に、要求登録点aが与えられたとき、そのauthPath(a)に含まれるレベルjのノード(j, a(j))の割り当て値V(j, a(j))を計算する手順 COMPLETION_SUB1を図66に示す(但し、0 ≦ j ＜ kでkは順次集約木の高さ)。これは、図70のステップS550aを中心に説明

するフローチャートである。

[0525] この手順で使用される変数及び関数は以下のとおりである。

[0526] ・chaindata0及びchaindata1はデータ構造chaindataを保持する変数である。

[0527] ・immedData1及びlateData1はデータ構造stackflmの線形リストを保持する変数である。

[0528] ・chaindata_storeは当該の集約期間における、各登録点において証明応答として受信したデータを格納する配列である。配列の各要素は、図64で定義したchaindataの構造を持つ。この配列のi番目の要素は、当該の集約間隔におけるi番目の登録点の即時補完データと、その直後の登録点で取得したi番目の登録点の遅延補完データを含む。

[0529] (1)本手順は2つの引数(入力)をもち、第1の引数を配列 chaindata_storeのindexを表す整数i0とし、第2の引数を順次集約木のレベルを表す整数jとする(ステップS5501a)。

[0530] (2)局所変数chaindata0にchaindata_store[i0]を設定し(ステップS5502a)、局所変数a0をchaindata1のleaf_index部とし(ステップS5503a)、変数a1にauthPath(a0)のレベルjのノードのindexを設定する(ステップS5504a)。

[0531] (3)図63に記述の認証パスノード割当値の取得参照点決定手順 DECIDE_POINT_AによりV(j, a(j))の取得参照点a2(要求登録点の1つで、その点で得られた連鎖補完データから、V(j, a(j))が計算できるもの)を決定する(ステップS5505a)。

[0532] (4)配列chaindata_storeを探索し、leaf_index部がa2であるような配列要素のindexとなる整数i1を決定する (ステップS5506a)。

[0533] (5)変数chaindata1にchaindata_store[i1]を設定する(ステップS5507a)。

[0534] (6)変数rgt_val1にchaindata1のrgt_val部を、変数immedData1に chaindata1のimmediate部を, 変数lateData1にchaindata1のlate部を、各々設定する(ステップS5508a)。

(7)rgt_val1、immedData1、あるいはlateData1にplace部が(j, a1)となるスタックフレームが含まれるかどうか判定する(S5509a)。

[0535] (7－1)含まれれば、その値を返す(ステップS5510a)。

[0536] (7－2)含まれないときは、immedData1とlateData1から、ハッシュ関数を介して計算できるノードの割当値をレベル0からレベルjまで順次計算する(ステップS5511a)。

[0537] (7－2－1)上記で順次計算された割り当て値に V(j, a(j))が含まれるか否か判定する(ステップS5512a)。

[0538] (7－2－1－1)含まれれば、その値を返す(ステップS5513a)。

[0539] (7－2－1－2)含まれなければ、エラーとする(ステップS5514a)。

[0540] 図67は、要求登録点aが与えられたとき、そのauthPath(a)に含まれるレベルjのノード(j, a(j))の割り当て値V(j, a(j))のリスト

[V(0, a(0)), V(1, a(1)), …, V(k－1, a(k－1))]

を計算する手順COMPLETION_SUB1を表す(但し、0 ≦ j ＜ kでkは順次集約木の高さ)

この手順で使用される変数及び関数は以下のとおりである。

[0541] ・kを順次集約木の高さとする。

[0542] ・auth_node_valsは長さkの配列で、各配列要素はハッシュ値を保持するものとする。

[0543] まず、図66のCOMPLETION_SUB1を各j (0≦j＜k)に適用し、authPath(a) に属する各ノードの割当値を計算し、計算結果をauth_node_vals[j]に格納する(ステップS5523a, S5524a)。

[0544] 次に、auth_node_valsを返り値とし、終了する(ステップS5525a)。

[0545] (インクリメンタル一括完全化)

上述したインクリメンタル完全化の方法は、完全化の対象となる受理証明書を指定し、その指定された受理証明書の個別完全化を行う方法である。次に述べるインクリメンタル完全化の方法は、ある利用者装置5Iが連続して取得した一連の受理証明書を一括して、上記のインクリメンタル個別完全化により計算されるものと同じデータを計算する方法である。この種類のインクリメンタル完全化をインクリメンタル一括完全化と呼ぶ。即ち、一連の登録点a(0), a(1), …, a(n)全てに対して上記のインクリメンタル個別完全化により計算されるものと同じデータを一括して計算することを、インクリメンタル一括完全化という。

[0546] インクリメンタル一括完全化は、上述した完全化波及処理を用いた以下の手順によ

り実行できる。

[0547] (1)a(0), …, a(n)を、ある集約間隔Iに属する、ある利用者装置5Iによる一連の登録点とする。

[0548] (2)利用者装置5Iによるa(n)の次の登録点をafとする。afは追伸点であってもよい。

[0549] (3)図68で記述した手順COMPLETION_BULK_BACKWARD1により、各a = a(n), …, a(0)を、この順にインクリメンタル完全化を行う。

[0550] この手順により、各登録点a(n－i)(但しi＝0, …, n)に対してafを暫定終端点とした場合のインクリメンタル個別完全化が実現されることが、以下のように数学的帰納法により示される(図69及び図70を参照)。以下では、簡単のためa(0), …, a(n)が共通の順次集約小木ST2に属し、afはST2の各リーフよりも右に位置する場合を考える。尚、一般の場合も同様である。

[0551] i＝0, …, nについて、手順COMPLETION_BULK_BACKWARD1により追加されたものを含むa(n－i)の遅延補完データと、a(n－i)で受信した即時補完データの合併は、a(n－i)のST2における全ての認証パスノードの割当値を含んでいることを示せばよい。

[0552] (1)帰納法のベース

i＝0のときを考える。このとき、a(n－i) = a(n)である。手順COMPLETION_BULK_BACKWARD1により、a(n)に対してはafの登録処理の終了時点におけるa(n)の遅延遅延補完データが追加される(図68のステップS5003a)。ここで、afの登録処理の終了時点においては順次集約小木のルート値は確定しているので、手順COMPLETION_BULK_BACKWARD1により追加されたものを含むa(n)の遅延補完データと、a(n)で受信した即時補完データの合併は、a(n)のST2における全ての認証パスノードの割当値を含んでいる。

[0553] (2)帰納ステップ

i1 ∈ {0, …, n－1}とし、i = i1としたとき、手順COMPLETION_BULK_BACKWARD1により追加されたものを含むa(n－i)の遅延補完データと、a(n－i)で受信した即時補完データの合併は、a(n－i)のST2における全ての認証パスノードの割当値を含んでいるものと仮定する。i ＝i1＋1に対しても同じことが成立つことを示せばよい。このことは、以下のように完全化波及処理を用いることにより示すことができる。

[0554] a2 = a(n－i1), a1 = a(n－(i1＋1))とおき、a1のa2による認証点を AP(a1, a2)、その兄弟ノードをAP'(a1, a2)、さらにAP(a1, a2)のレベルをj1と置く(図70を参照)。

[0555] 以下で述べる順次集約木の性質により、順序集約小木ST2におけるa1のST2における認証パスノードのうちレベルがj1より小さいもの割当値は、図68のステップS5004aにおいて追加されるデータに含まれる。

[0556] a1のST2における認証パスノードのうちレベルがj1に等しいものの割当値は、図68のステップS5007aにおいて追加されるデータに含まれる。

[0557] a1のST2における認証パスノードのうちレベルがj1より大きいものの割当値は、図68のステップS5008aにおいて追加されるデータに含まれる。

[0558] 以上により、手順COMPLETION_BULK_BACKWARD1により追加されたものを含む a1 = a(n－(i＋1))の遅延補完データとa(n－(i＋1))で受信した即時補完データの合併は、a(n－(i＋1))のST2における全ての認証パスノードの割当値を含むことが導かれる。

[0559] 以上(1)及び(2)により、i＝0, …, n について、手順COMPLETION_BULK_BACKWARD1により追加されたものを含むa(n－i)の遅延補完データと、a(n－i)で受信した即時補完データの合併は、a(n－i)のST2における全ての認証パスノードの割当値を含んでいることが示される。

[0560] なお、同様の帰納法により、図68のステップS5006aで判定結果が NO となり、エラーとなることはないことも示される。

[0561] (メモリの効率化)

上記は、1つの集約間隔において連鎖補完方式により利用者装置5Iがイベント順序証明応答として取得したデータを計算機のメモリに読み込むことができるできる場合の処理方式である。集約間隔における利用者装置5Iによる登録点が多数に上り上記の取得データを計算機のメモリに読み込むことができない場合には、以下の方式により取得データの一部をメモリに読み込み、完全認証パスデータを段階的に計算することにより、当該の集約間隔における全ての登録点の完全認証パスデータを計算することができる。

[0562] 上記の計算は、以下のステップ(1)～(5)により行われる。

[0563] (1)ある集約間隔にある利用者装置5Iが受信した補完データのうちから、登録点のインデックスが特定の条件を満たすもののみを間引き抽出し、間引き抽出データを構成する。

[0564] 間引き抽出するための条件として、間引き間隔となる正整数mを指定し、登録点のインデックスがmで割り切れるもののみを抽出することにしてもよい。図71に示す具体例においては、インデックス 0から10までをもつ登録点(黒い点で示されている)から、間引き間隔を5として、5で割り切れるインデックス即ち0, 5,10を持つ登録点を抽出し、間引き抽出データを構成している。

[0565] (2)登録点のインデックスが隣あう間引き抽出データのインデックスで挟まれているような登録点の登録値および補完データからなる局所データを構成する。このような局所データは、一般には複数構成される。

[0566] 図72に示す具体例においては、間引き抽出データの1番目のインデックス0と2番目のインデックス5に挟まれたインデックスを持つ登録点を集め第1の局所データを構成している。図73に示す具体例においては、間引き抽出データの2番目のインデックス5と3番目のインデックス10に挟まれたインデックスを持つ登録点を集め第2の局所データを構成している。

[0567] (3)上記(2)で構成された各局所データを、その局所データの最も右に位置する登録点を暫定終端点として扱い、前記のインクリメンタル完全化の処理を行う。この処理を局所データの局所完全化と呼ぶ。

[0568] この処理により計算される遅延補完データを用いて、当該の局所データに属する登録点のうち最も右に位置するものをa1としたとき、当該の局所データに属する各登録点aについて、aのa1による認証点をAP(a, a1)としたとき, aの認証パスノードの中で、level(AP(a, a1))より低いレベルのものに対しては、その割当値を計算することができる。さらに、ここで割当値を計算できるaの認証パスノードの割当値は、aの認証パスノードのうちa1の処理が終了した時点で割当値が定まっているもの全てを含んでいる。即ち、登録点aのa1時点の遅延補完データを含んでいる。

[0569] 図72に示す具体例においては、この局所データの局所完全化の処理により、インデックス0の登録点の遅延補完データとして、ノード(1, 0), (2, 1) の割当値が計算さ

れ、インデックス1の登録点の遅延補完データとして、ノード(2, 1)の割当値が計算され、インデックス3の登録点の遅延補完データとして、ノード(1, 5)の割当値が計算される。

[0570] この局所データに属する登録点のうち最も右に位置するものはインデックス5の登録点でありこれをa1と置くと、この局所データに属する各登録点aについて、level(AP(a, a1))より小さいレベルの認証パスノードの割当値が計算できる。例えば、aをインデックス0の登録点とすると、AP(a, a1) は(3, 0)であり、aの認証パスノードのうちレベルが3より小さいもの(0, 0), (1, 0), (2, 1)の割当値を計算できる。aのa1における遅延補完データは(1, 0), (2, 1)の割当値であるので、a1時点における遅延補完データは計算できることがわかる。この局所データに属する他の登録点についても同様である。

[0571] (4)上記(3)の処理の結果、間引き抽出データの隣あう2つの登録点a1とa2について、a1のa2時点における遅延補完データを取得することが出来る。このデータを用いて前記の証明書完全化のメインルーチン COMPLETION_MAIN1を適用し、間引き抽出データに含まれる各登録点で取得する証明書の完全化、即ち該登録点の全ての認証パスノードの割当値を計算する。この処理を間引き抽出データの大域完全化と呼ぶ。

[0572] 図74で示す具体例においては、間引き抽出データのインデックス0, 1, 2の登録点、即ち、リーフ番号1, 11, 3の登録点の証明書の完全化を行い、当該の3つの登録点の全ての認証パスノードの割当値を計算することができる。例えば、間引き抽出データのインデックス0の登録点の認証パスノードは (0, 0), (1, 1), (2, 1), (3, 1), (4, 1)であるが、これら全ての割当値を計算することができる。

[0573] (5)上記(3)で構成した局所完全化された局所データの各々と、上記(4)で構成した大域完全化された間引き抽出データを用いて、当該の局所データに含まれる各登録点で取得する証明書の完全化を行う。この処理を局所データの大域完全化と呼ぶ。

[0574] 局所データの大域完全化の手順は、詳しくは以下の通りである。

[0575] (5－1)ある局所データの登録点をa(0), a(1), …, a(n) = a1とするとき、a1の全ての認証パスノードの割当値は、ステップ(4)で計算済みである。これを、

V(0), V(1), …, V(k－1) とする。

[0576] (5－2)従って、a1のルートパスに属する各ノードの割当値も計算できる。これを V'(0), V'(1), …, V'(k－1), V'(k) とする。

[0577] (5－3)各a = a(0), …, a(n－1)について、aのa1による認証点をAP(a, a1)とし、k1 = level(AP(a, a(n))とおく。

[0578] (5－4)ステップ(3)により、aの認証パスノードのうちレベルがk1より小さいものの割当値は計算可済みである。

[0579] (5－5)また、レベルがk1のaの認証パスノードはa1のルートパスに属するノードでレベルがk1のものと一致する。従って、このような認証パスノードの割当値は、上記(5－2)で計算したV'(k1)となる。

[0580] (5－6)k1 < j < kとなるjについて、aの認証パスノードのうちレベルがjのものは、a1の認証パスノードのうちのレベルがjのものと一致する。従って、その認証パスノードの割当値は、上記(5－1)で計算したV'(j)である。

[0581] 以上、(5－1)～(5－6)により、各a = a(0), …, a(n－1)についてaの全ての認証パスノードの割当値を計算することが出来る。

[0582] 図72で示す具体例について言えば、インデックス2の登録点(リーフ識別番号5)の認証パスノードは、(0, 4), (1, 3), (2, 0), (3, 1), (4, 1) である。またa1をインデックス5の登録点(リーフ識別番号11)とすると、AP(a, a1) = (3, 0)であり、k1 = level(AP(a, a1)) = 3である。aの認証パスノードのうちレベルがk1 = 3より小さい(0, 4), (1, 3), (2, 0)についてはそれらの割当値は、上記ステップ(5－3)で計算できる(図72、図75参照)。また、レベルがk1 = 3の認証パスノード(3, 1)の割当値は(5－2)で計算できる(図74、図75参照)。また、レベルがk1 = 3より大きい(4, 1)についてはステップ(5－1)で計算できる(図74、図75参照)。

以上のステップ(1)～(5)の手順により、取得した証明書の完全化を行うために、同時にメモリ上に保持する必要のあるデータは、間引き抽出データと、一つの局所データのみである。登録点の総数をNとし，上記ステップ(1)で用いる間引き間隔をmとすると、同時にメモリ上に保持する必要がある登録点の数は、(N/m)＋mとなる。m = √Nとすると、(N/m)＋m = 2・√Nとなり、必要なメモリ容量のオーダをNから√Nに削減

することが可能となる。

[0583] ＜5－5．利用者装置5Iの補完データによるルート値計算＞

次に、利用者装置5Iの補完データによるルート値計算について、説明する。これは、利用者装置5Iの第1の検証機能におけるルート値計算について詳しく説明するものである。

[0584] ある集約間隔I1が終了したとき、利用者装置5Iは、集約間隔I1の間に送信した1つの証明要求RQに対する受理証明書の個別完全化を上述の方法で実行することにより、完全認証パスデータを計算することができる。完全認証パスデータから、以下に示す(1)～(5)に示す手順により、当該の集約間隔の順次集約木のルートの割当値が計算できる。

[0585] まず完全認証パスデータは、即時補完データと遅延補完データからなる。即時補完データや遅延補完データは、(位置情報, LRタグ, 割当値(ハッシュ値))で示す形式の補完データ要素からから成るものとする。尚、LRタグはLというタグかRというタグのどちらかの値をとる。ここで、上記の位置情報はレベル情報を含むものとする。レベル情報の間には以下のような2項関係＜＜が定義されているものとする。

[0586] 任意の登録点について、その完全認証パスデータに含まれる補完データ要素を

(位置情報P(i), LRタグT(i), 割当値H(i)) (但し, i ＝1, …, n)

とし、位置情報P(i)に含まれるレベル情報をlevel(P(i))と表すと、2項関係＜＜は

level(P(1)), …, level(P(n))

の間に線形順序を定義するものとする。

[0587] 位置情報を1つの集約木におけるレベル(非負整数で表される)とレベル内のインデックスの組み合わせとし、位置情報のうちレベル情報は組み合わせの第1要素とすると、上記2項関係＜＜としては、整数の大小関係＜をとればよい。

[0588] 図76は、完全認証パスデータによる順次集約木のルート値の計算方法を示すフローチャートである。同図によれば、完全認証パスデータのチェック、即ち、即時補完データはLタグ、遅延補完データはRタグを有するかのチェック、及び完全認証パスデータに重なるレベル情報がないかのチェックを確認した後、レベル情報の順序でソートし、各割当値をLRタグに合わせて連接して、ルート値を計算する(ステップS3101

a, S3102a, S3103a, S3104a, S3105a, S3106a)。

[0589] 次に、図77及び図78に示すように、ある集約間隔の順次集約木のリーフの1つとして、前の集約間隔の順次集約木のルート値を取り入れる場合について説明する。このような場合には、異なる順次集約木間における受理証明書発行の時間的前後を検証することが簡単にできるという効果がある。例えば、図78において、利用者装置2Aの登録点aが順次集約木ST(5)の部分木ST1(5)のリーフに割り当てられており、また、利用者装置2Bの登録点bが順次集約木ST(6)の部分木ST1(6)のリーフに割り当てられているときは、aとbの合流点がノードR(6)、aのbによる認証点がノードR(5)になるので、登録点aから計算された認証点R(5)の値が、登録点bの即時補完データに含まれていれば、登録点aの登録は登録点bの登録より時間的に前であることを検証することができる。

[0590] 図77は、図78のように複数の順次集約木がリンクされた状況において、1つの順次集約木ST(n)を抽出したものである。

[0591] ここで、ルートR(n-1)は、順次集約木ST(n－1)と順次集約木ST(n)に共通するノードで、

レベル情報(L, TID(n－1), k(n－1))

レベル内index 0

位置情報((L, TID(n－1), k(n－1)), 0)

である。尚、上述のレベル情報は、

(LRタグ, 非負整数の集約木番号, 非負整数の集約木内のレベル情報)

で表現されており、LRタグは、Lというタグ とRというタグのどちらかの値をとる。

[0592] また、部分木ST1(n)のルートR1(n)は、

レベル情報(R, TID(n－1), k1(n))

レベル内index 1

位置情報((R, TID(n－1), k1(n)), 1)

であり、ここで、k1(n)はST1(n) の高さである。

[0593] また、部分木ST1(n)に関しては、ルート R1(n)以外のノードについては、

レベル情報(R, TID(n), j)

ルートR1(n)以外のノードの位置情報は((R, TID(n), j), i) である。

[0594] ここで, j, iは非負整数であり、leafs(ST1(n))の各要素の位置情報は((R, TID(n), 0), i) と表すことができる。

[0595] また、R(n)は順次集約木ST(n)とST(n+1)に共通するノードで、

レベル情報(L, TID(n), k(n))

レベル内index 0

位置情報 ((L, TID(n), k(n)), 0)(但し、k(n) = k1(n)+1とする)

割当値V(R(n)) = h(V(R(n−1)) || V(R1(n)))

である。

また、順次集約小木ST1(n)とルートR(n−1)、ルートR(n)からなる二分木をST(n)と書く。即ち、

root(ST(n)) = R(n)、

leftChild(R(n)) = R(n−1)、

rightChild(R(n)) = R1(n)。

[0596] 第n番目の集約期間に対応する順次集約木はST(n)である。

[0597] 但し、n = 0に対しては、R(n−1)の代わりに所定の割当値を持ったノードIRを用いる(図78参照)。IRの位置情報は((L, −1, 0), 0) である。

[0598] このとき、2つの 拡張レベル情報の間の順序<<を次のように定義する。

[0599] ∀j1, j2, T1, T2 ≧ 0 [(R, T2, j2) << (L, T1, j1)] 、

∀j1, j2, T1, T2 ≧ 0 [T1 < T2 ⇒ (L, T1, j1) << (L, T2, j2)]、

∀j1, j2, T1 ≧ 0 [j1 < j2 ⇒ (R, T1, j1) << (R, T1, j2)]。

[0600] この定義により、二項関係<<は任意の登録点の認証パスノードの集合に線形順序を定めるものであることが導かれる。

[0601] 図79は、この定義された2項関係<<を用いて補完データによる集約木ルート値を計算する一例を示すもので、計算は以下のようになる。

[0602] 位置情報((R, 10, 0), 5) のノードに対して、即時補完データは、

[(((L, 9, k(9)), 0), L, V(R(9))),

(((R, 10, 2), 0) , L, V((R, 10, 2), 0)),

(((R, 10, 0), 4), L, V((R, 10, 0), 4))]

となる。ここで(R, 10, 2) << (L, 9, 10) である。

[0603] 遅延補完データは、[(((R, 10, 1), 3), R, V((R, 10, 1), 3))]

補完データからのルート値の計算を図76のフローに従って行う。

[0604] (1)即時補完データの各要素はLタグを持つことをチェックする → 合格

(2)遅延補完データの各要素はRタグを持つことをチェックする → 合格

(3)即時補完データと遅延補完データを合併する

合併結果は、

[(((L, 9, k(9)), 0), L, V(R(9))),

(((R, 10, 2), 0), L, V((R, 10, 2), 0)),

(((R, 10, 0), 4), L, V((R, 10, 0), 4)),

(((R, 10, 1), 3), R, V((R, 10, 1), 3))]

となる。

[0605] (4)合併結果の中に、重なるレベル情報がないことを確認する → 合格

(5)合併結果を、レベル情報の順序 << 基準にソートする

ソート結果は,

[(((R, 10, 0), 4), L, V((R, 10, 0), 4)),

(((R, 10, 1), 3), R, V((R, 10, 1), 3)),

(((R, 10, 2), 0), L, V((R, 10, 2), 0)),

(((L, 9, k(9)), 0), L, V(R(9)))]

となる。

[0606] (6)ステップ(5)のソートの結果を

(J(0), LR(0), V(0)), …, (J(k−1), LR(k−1), V(k−1))

とおき、当該の登録点の登録値をV(0)とおき、以下のように再帰的に

W(0), W(1), …, W(k−1), W(k)

を定義する。

[0607] (i)W(0) = V(0)

(ii)LR(j) = Lのとき、W(j+1) = h(V(j) || W(j))

LR(j) = R のとき、W(j+1) = h(W(j) || V(j))

これに従って計算すると、k = 4であり、W(j) は以下のように計算できる。

[0608] W(0) = V((R, 10, 0), 5),

W(1) = h(V((R, 10, 0), 4) || V((R, 10, 0), 5)),

W(2) = h(W(1) || V((R, 10, 1), 3)),

W(3) = h(V((R, 10, 2), 0) || W(2)),

W(4) = h(V(R(9)) || W(3))

となる。W(3) = V(R1(10)), W(4) = V(R(10))である。

[0609] 従って、第5の実施の形態のイベント順序証明システム200aによれば、第4の実施の形態と同じ効果を得ることができる。即ち、木構造を用いてイベント順序を証明するイベント順序証明システムにおいて、利用者装置5Iから証明要求を受付けた証明装置4aが、該証明要求に対して受理証明書を含む連鎖補完方式(登録点に関して、登録点の即時補完データ及び直前登録点の登録点における遅延補完データを証明応答データに含む)による証明応答を発行したときでも、利用者装置5Iがこの証明応答を用いて、インクリメンタル完全化を行うと、利用者装置5I間における受理証明書発行の時間的前後を検証することができるので、証明要求をまとめた公表データが電子的に公表される前であっても、受理証明書の正当性を検証することができる。

[0610] また、連鎖補完方式には、シーケンス補完方式よりも、証明応答のデータ量が少なくて済むという効果がある。さらには、連鎖補完方式においても、証明装置4aは、順次集約木そのものを記憶部に記憶させる方法は勿論、スタック構造を用いた記憶方法も用いることができるので、証明装置4aの必要記憶容量を大幅に減少させることもできる。

[0611] また、利用者装置5Iにおけるインクリメンタル完全化処理においても、個別完全化及び一括完全化の双方を具備するので、状況に応じて最適なインクリメンタル完全化を行うことにより、受理証明書の正当性を検証することができる。さらに、証明応答データすべてを利用者装置5Iのメモリ上に記憶させず、部分的な局所データだけを記憶させる方式であっても、インクリメンタル完全化を行うことができるので、利用者装置5Iの必要なメモリ量を大幅に減少させることができる。

[0612] また、順次集約期間が終了後においては、利用者装置5Iは、インクリメンタル完全化の処理により、完全補完データを取得できるので、順次集約木のルート値を計算することができる。さらに、前の集約間隔の順次集約木のルート値を次の順次集約木のリーフの割当値とする場合には、順次集約木をまたがった受理証明書発行の時間的前後を検証することが簡単にできる。

[0613] 以上、本発明の実施例について説明してきたが、本発明の要旨を逸脱しない範囲において、本発明の実施例に対して種々の変形や変更を施すことができる。例えば、上記実施の形態においては、順次集約木として二分木を用いたが、本発明は二分木に限定されるものではなく、1つの親が複数の子を持つ有向木であればよいものである。

[0614] また、利用者装置2I又は5Iは、一定時間間隔終了前に、証明装置1a又は4aが運用を中断、あるいは順次集約木のルート値を計算するのに必要なデータを消失したとき、証明装置1a又は4aの運用中断あるいはデータ消失の時点までに受信し記憶した順序証明応答から、計算可能な割当値を持つ順次集約木のノードのうちで、その親のノードの割当値が計算できないような1つあるいは複数のノードの位置情報と割当値を、電子的に公表する利用者サイド電子的情報公表手段を有してもよい。そして、この場合、所定の検証機関が、この公表情報が矛盾しないことを検証するようにしてもよい。

[0615] ＜順次集約木の性質＞

第4及び第5の実施の形態で用いた順次集約木の性質について詳しく説明する。

[0616] 順次集約木のリーフ番号iについて、iで識別される順次集約木のリーフに順次割当値を割り当てる元となった証明要求を受付けて該リーフに割当値を割り当てる一連の処理を該リーフに対する処理ラウンドと言いround(i)と表す。

[0617] 今、甲を利用者装置、乙を監査装置とし、i0とi1をi0 ＜ i1なる二つの順次集約木リーフ番号とし、round(i0)において甲は受理証明書を受信し、乙 はround(i1)において監査用受理証明書を受信したものとする。このとき、i0のi1による認証点は以下の性質を持つ。

[0618] (1)認証点の割当値は、監査点、即ちノード(0, i1)の即時補完データに含まれる。

[0619] (2)上記認証点を(j', i')とおき、round(j1)終了時にリーフ(0, i0)が属する順次集約小木をST2とし、(0, i0)のST2における認証パスをauthPathST2(0, i0))としたとき、authPathST2(0, i0))に属するノードで、レベルがj'より小さいものに対する割当値は、ノード(0, i0)に対応するラウンドで受理証明書を受理した利用者が、ノード(0, i1)に対応するラウンド以降において受信できる遅延補完データあるいは受信した即時補完データに含まれる。

[0620] 即ち、i1 ≦ i2とすると、authPathST2(0, i0))に属するノードで、レベルがj'より小さいものに対する割当値は、immedData(i0)あるいはlateData(i0, i2)に含まれる。

[0621] (3)ST2におけるリーフ(0, i0)のルート・パスをrtPathST2(0, i0)としたとき、上記認証点の割当値及びにrtPathST2(0, i0)属するノードでレベルが該認証点のレベルより小さいノードの割当値は、ノード(0, i0で受理証明書を受理した利用者が、ノード(0, i1)に対応するラウンド以降において受信する遅延補完データおよびノード(0, i0)で受信した受理証明書(即時補完データを含む)から計算することができる。

[0622] (性質の証明)

以下では、利用者に渡す受理証明書に、即時補完データを含める場合について説明する。利用者に渡す受理証明書に即時補完データを含めず、その代わりに遅延補完データにこの情報を含める場合でも同様の議論により同じ結論が得られる。

[0623] (1)まず、項目(1)について図80、図81を用いつつ説明する。

[0624] (場合1)最初に、図80を参照して、i0とi1がi1時点における順次集約フォレスト内の1つの順次集約小木ST2に属する場合を考える。ここで、合流点を(j, i)、そのレフト・チャイルドである認証点を(j', i')とおく。ノード(0, i1)の順次集約小木ST2におけるルート・パスrtPathST2(0, i1)において、(0, i1)から出発して、合流点に至る直前のノードを(j″, i″)とおく。このとき、認証点は、(j″, i″)の左補完点である。従って、認証パスauthPathTST2(i1)の定義から、((j', i'), L)はノード(0, i1)のST2における認証パスに含まれる。また、ノード(j', i')への値の割当ては、round(i1)より前に終了している。よって、((j', i'), L, V(j', i'))は(0, i1)に対する即時補完データに含まれる。

[0625] (場合2)次に、図81を参照して、i0とi1がi1時点における順次集約フォレスト内のどの順次集約小木にも同時には属さない場合を考える。このとき、i0はi1時点における

順次集約フォレスト内のある順次集約小木ST2'に属する。このとき、登録点(0, i1)に対する即時補完データの定義により、V(root(ST2'))は、登録点(0, i1)に対する即時補完データに含まれる。

[0626] (2)次に項目(2)について図82乃至85を用いつつ説明する。

[0627] (場合1)最初に、図82及び83を参照して、i0とi1がi1時点における順次集約フォレスト内の1つの順次集約小木ST2に属する場合を考える。

[0628] k = height(ST2)とおく。

[0629] 認証点(j', i')はノード(0, i0)のルート・パスrtPathST2(0, i0)に含まれる。ここで、

rtPathST2(0, i0) = [(0, r(0)), ⋯, (j', r(j')), (j'+1, r(j'+1)), ⋯, (k, r(k))]

とする。また、authPathST2(0, i0)の要素で、レベルがj'より小さいノードの並びを

[(0, s(0)), ⋯, (j'−1, s(j'−1))]

とおく。各j1 ∈ [0..j'−1]に対して、V(j1, r(j1))がimmedData(i0)あるいはlateData(i0, i2) に含まれることを示せばよい。

[0630] authPathST2(0, i0)の定義により、authPathST2(0, i0)のレベルj1の要素p2 = (j1, s(j1))は、rtPathST2(0, i0))のレベルj1+1の要素p3 = (j1+1, r(j1+1))のライト・チャイルドであるか或いはレフト・チャイルドである。どちらであるかによって場合分けする。

[0631] (場合1−1)p2がp3のライト・チャイルドであるとき、図82に示すように、p2の割当値V(p2)は、i1 ≦ i2なるi2において、甲が受信できる遅延補完データlateData(i0, i2)に含まれる。なぜならば、リーフ(0, i1) に対応するラウンドのイベント順序証明処理が終わった時点で、図82のBで表されたSB2の部分木の割当値は計算可能であり計算され割当て済みである。従って、その時点以降で発行される登録点i0に対する遅延補完データにはBのルートp2の割当値V(p2)が含まれるからである。

[0632] (場合1−2)p2がp3のレフト・チャイルドであるとき、図83に示すように、ノードp2の割当値V(p2)は、登録点i0に対する即時補完データに含まれる。何故ならば、図83のp1をルートとする部分木Bについて、

∀I ∈ leafs(B)[i < i0]

であり、従ってi0で識別されるラウンドの開始時に、leafs(B)の割当値は確定している。よって、p2 = root(B)の割当値は、i0で識別されるラウンドにおいて確定しており、従

ってp2はi0時点において値が確定しているi0の認証パスノードの集合に含まれるからである。

[0633] (場合2)次に、図84及び図85を参照して、i0とi1がi1時点における順次集約フォレスト内のどの順次集約小木にも同時には属さない場合を考える。このとき、i0はi1時点における順次集約フォレスト内のある順次集約小木ST3に属し、root(ST3)がi0のi1による認証点となる。k =height(ST3)と置く。認証点(j', i')は(0, i0)のルートパスrtPathST3(0, i0)に含まれる。ここで、

rtPathST3(0, i0) = [(0, r(0)), ⋯, (j', r(j')), (j'+1, r(j'+1)), ⋯, (k, r(k))]

とする。また、authPathST3(0, i0)の要素で、レベルがj'より小さいノードの並びを

[(0, s(0)), ⋯, (j'−1, s(j'−1))]

とおく。各j1 ∈ [0..j'−1]に対して、V(j1, r(j1))がimmedData(i0)あるいはlateData(i0, i2)に含まれることを示せばよい。

[0634] authPathST3(0, i0)の定義により、authPathST3(0, i0)のレベルj1の要素p2 = (j1, s(j1))は、rtPathST3(0, i0))のレベルj1+1の要素p3 = (j1+1, r(j1+1))のライト・チャイルドであるか或いはレフト・チャイルドである。どちらであるかによって場合分けする。

[0635] (場合2−1)p2がp3のライト・チャイルドであるとき、図84に示すように、p2の割当値V(p2)は、i1 ≦ i2なi2において、甲が受信できる遅延補完データlateData(i0, i2)に含まれる。なぜならば、リーフ(0, i1)に対応するラウンドのイベント順序証明処理が終わった時点で、図84のBで表されたSB3の部分木の割当値は計算可能であり計算され割当て済みであり、従ってその時点以降で発行される登録点i0に対する遅延補完データにはBのルートp2の割当値V(p2)が含まれるからである。

[0636] (場合2−2)p2がp3のレフト・チャイルドであるとき、図85に示すように、ノードp2の割当値V(p2)は、登録点i0に対する即時補完データに含まれる。何故ならば、図85のp1をルートとする部分木Bについて、

∀i ∈ leafs(B)[i < i0]

であり、従ってi0で識別されるラウンドの開始時に、leafs(B)の割当値は確定している。よって、p2 = root(B)の割当値は、i0で識別されるラウンドにおいて確定しており、従ってp2はi0時点において値が確定しているi0の認証パスノードの集合に含まれるから

である。

[0637] (3)認証パスの定義及び項目(2)から、各j1 ∈ [0..j']に対して、V(j1, (j1))を以下のように再帰的に計算することが出来る。

[0638] まず、V(j1, r(j1))は受理証明書に含まれているノード(0, i0)の割当値とする。

[0639] 次に、j1 ∈ [0..j'－1]に対して、V(j1, r(j1)) が計算されたと仮定し、V(j1+1, r(j1+1))を以下のように計算する。r(j1) < s(j1)のときは、

$$V(j1+1, r(j1+1)) = h(V(j1, r(j1)) \| V(j1, s(j1)))$$

とし、s(j1) < r(j1) のときは、

$$V(j1+1, r(j1+1)) = h(V(j1, s(j1)) \| V(j1, r(j1)))$$

とする。

産業上の利用可能性

[0640] 本発明によれば、木構造を用いてイベント順序を証明するイベント順序証明システムにおいて、イベント順序証明要求をまとめた公表データを用いなくても、イベント順序証明機関から発行されたイベント順序受理証明書の検証を行うことができる。

[0641] この結果、公表期間の途中であっても、受け取ったイベント順序受理証明書の正当性を検証することができ、利用者の利便性の向上を図ることができる。また、イベント順序証明機関に障害が発生しても、障害に強いイベント順序証明システムを構築することができる。

請求の範囲

[1] 所定のデジタル情報を生成するイベントの時系列において、あるイベントを生成した相対的な時刻、即ち時間的順序、を証明する証明要求を行う利用者装置と、前記利用者装置からの前記証明要求に対する証明書を作成する証明装置と、前記証明書の真偽を監査する監査装置とが通信ネットワークを介して相互に接続されたイベント順序証明システムにおけるイベント順序証明方法であって、

前記証明装置が前記利用者装置からの証明要求を受信する順序証明要求受信ステップと、

前記証明装置が前記証明要求に含まれるデジタル情報から予め定めた手順に従って順次割当データを作成する順次割当データ計算ステップと、

前記証明装置が、一連の順次割当データを時刻順に有向木のリーフに左から順次割り当てることによって一定時間間隔ごとに1つの集約木が生成される順次集約木において、同一の親を有する複数の子に割り当てられたそれぞれの割当値を連接した連接値に所定の衝突困難一方向関数を適用した結果値を前記親の割当値とする計算方法により、計算可能なノードの割当値を計算するとともに、前記一定時間間隔終了後に前記順次集約木のルートに割り当てるルート値を計算する順序証明要求集約ステップと、

前記証明装置が、前記順次割当データ、並びに前記順次割当データが割り当てられた順次集約木及び該順次集約木のリーフを特定する第1の順次集約木特定情報を含む証明書を作成する証明書作成ステップと、

前記証明装置が前記証明書を前記利用者装置に送信する証明書送信ステップと、

前記証明要求が割り当てられた前記順次集約木のリーフを登録点と定義し、該登録点から前記順次集約木のルート値を計算するのに必要なノードに関する情報を前記証明書の補完情報と定義し、該補完情報のうち、前記証明要求を前記順次集約木に割り当てた時点において取得可能な補完情報を即時補完情報と定義すると、

前記証明装置が、前記証明要求を前記順次集約木に割り当てた以後に、第1の監査要求を前記順次集約木に割り当て、前記証明書と同一の作成方法により、第1の

監査用証明書を作成するとともに、前記監査要求を前記順次集約木に割り当てた時点における第1の監査用の即時補完情報を前記順次集約木から取得し、前記第1の監査用証明書に含める監査用証明書作成ステップと、

前記証明装置が前記第1の監査用証明書を前記監査装置に送信する監査用証明書送信ステップと、

前記証明装置が、前記第1の監査要求を前記順次集約木に割り当てた以後に、前記利用者装置からの前記証明書の補完情報の要求を受信する補完情報要求受信ステップと、

前記証明装置が、前記補完情報の要求が割り当てられた前記順次集約木及び前記順次集約木のリーフを特定する第2の順次集約木特定情報、及び前記補完情報の要求を割り当てた時点において取得可能な補完情報を前記順次集約木から取得し、遅延補完情報とする遅延補完情報作成ステップと、

前記証明装置が前記証明書の前記遅延補完情報を前記利用者装置に送信する遅延補完情報送信ステップと、

を有することを特徴とするイベント順序証明方法。

[2] 前記証明書作成ステップにおいて、前記証明装置は、前記第1の順次集約木特定情報に前記証明書の即時補完情報を含めることを特徴とする請求項1記載のイベント順序証明方法。

[3] 前記監査用証明書作成ステップは、さらに、前記証明装置が、前記証明要求を前記順次集約木に割り当てた以前に、第2の監査要求を前記順次集約木に割り当て、前記証明書と同一の作成方法により、第2の監査用証明書を作成するとともに、前記第2の監査要求を前記順次集約木に割り当てた時点における第2の監査用の即時補完情報を前記順次集約木から取得し、前記第2の監査用証明書に含めるステップを備え、

前記証明装置が、前記一定時間間隔終了後に前記監査用証明書作成ステップで作成された各監査用証明書の補完情報すべてを前記順次集約木から取得し、各監査用証明書の遅延補完情報とする監査用遅延補完情報作成ステップと、

前記証明装置が前記第1及び第2の監査用証明書の前記遅延補完情報を前記監

査装置に送信する監査用遅延補完情報送信ステップと、

をさらに有することを特徴とする請求項1又は2記載のイベント順序証明方法。

[4] 前記順次割当データ計算ステップにおいて、前記証明装置は、前記証明要求に含まれる前記デジタル情報に対して所定の衝突困難一方向関数を適用した結果値を前記順次割当データとして計算することを特徴とする請求項1乃至3のいずれか1項に記載のイベント順序証明方法。

[5] 前記証明書作成ステップにおいて、前記証明装置は、前記証明書にデジタル署名を施すことを特徴とする請求項1乃至4のいずれか1項に記載のイベント順序証明方法。

[6] 前記証明装置が、前記一定時間間隔終了後に前記順次集約木の前記ルート値を電子的に公表する電子的情報公表ステップをさらに有することを特徴とする請求項1乃至5のいずれか1項に記載のイベント順序証明方法。

[7] 前記利用者装置から複数の証明要求が為されたときには、前記証明書送信ステップは、前記証明装置が、各証明要求を前記順次集約木に割り当てた時間的順序で、各証明要求に対する証明書を送信するステップをさらに有することを特徴とする請求項1乃至6のいずれか1項に記載のイベント順序証明方法。

[8] 前記利用者装置から複数の証明要求が為されたときに、

前記証明装置が前記順序証明要求集約ステップで生成される前記順次集約木に関する情報を記憶する順次集約木記憶ステップと、

前記順次集約木において、リーフa1より右に位置するリーフa2の割当処理が終了した時点で定まる前記リーフa1の遅延補完情報を、前記リーフa1の前記リーフa2における遅延補完情報といい、さらに、最新の証明要求から作成された順次割当データが割り当てられた前記順次集約木のリーフを新登録点とすると、

前記証明装置が前記複数の証明要求の登録点に関する情報を記憶する登録点記憶ステップと、

をさらに有し、

前記証明書作成ステップにおいて、前記証明装置は、各記憶ステップにおいて記憶された情報から、該新登録点の順次割当データと、該順次割当データが割り当て

られた前記順次集約木及び該順次集約木のリーフを特定する第1の順次集約木特定情報と、前記新登録点の即時補完情報と、前記利用者装置の過去のすべての登録点の前記新登録点における遅延補完情報と、を併せることによって前記新登録点に対する証明書を作成することを特徴とする請求項2記載のイベント順序証明方法。

[9] 前記利用者装置から複数の証明要求が為されたときに、

前記証明装置が前記順序証明要求集約ステップで生成される前記順次集約木に関する情報を記憶する順次集約木記憶ステップと、

前記順次集約木において、リーフa1より右に位置するリーフa2の割当処理が終了した時点で定まる前記リーフa1の遅延補完情報を、前記リーフa1の前記リーフa2における遅延補完情報といい、さらに、最新の証明要求から作成された順次割当データが割り当てられた前記順次集約木のリーフを新登録点とすると、

前記証明装置が前記新登録点に対する直前の登録点に関する情報を記憶する登録点記憶ステップと、

をさらに有し、

前記証明書作成ステップにおいて、前記証明装置は、各記憶ステップにおいて記憶された情報から、該新登録点の順次割当データと、該順次割当データが割り当てられた前記順次集約木及び該順次集約木のリーフを特定する順次集約木特定情報と、前記新登録点の即時補完情報と、前記利用者装置の前記直前の登録点の前記新登録点における遅延補完情報と、を併せることによって前記新登録点に対する証明書を作成することを特徴とする請求項2記載のイベント順序証明方法。

[10] 前記順次集約木記憶ステップにおいて、前記証明装置は、前記順次集約木に関する情報として、前記順次集約木において割当処理がされた各ノードの位置及び割当値を記憶することを特徴とする請求項8又は9記載のイベント順序証明方法。

[11] 前記証明装置は、前記新登録点の前記即時補完情報と、前記利用者装置の前記直前の登録点の前記新登録点における前記遅延補完情報とを別々にスタック化して記憶することを特徴とする請求項9記載のイベント順序証明方法。

[12] 前記証明装置が前記一定時間間隔終了後に前記順次集約木の前記ルート値を電子的に公表する電子的情報公表ステップをさらに有することを特徴とする請求項8乃

至11のいずれか1項に記載のイベント順序証明方法。

[13] 前記一定時間間隔終了前に、前記証明装置が運用を中断、あるいは前記順次集約木のルート値を計算するのに必要なデータを消失したときに、前記利用者装置が、前記証明装置の運用中断あるいはデータ消失の時点までに受信し記憶した証明書から、計算可能な割当値を持つ前記順次集約木のノードのうちで、その親のノードの割当値が計算できないような1つあるいは複数のノードの位置情報と割当値を、電子的に公表する利用者サイド電子的情報公表ステップをさらに有することを特徴とする請求項8乃至12のいずれか1項に記載のイベント順序証明方法。

[14] 前記順序証明要求集約ステップにおいて、前記証明装置は、前記一定時間間隔終了後に前記順次集約木の前記ルート値を、次の順次集約木のリーフに割り当てられた新たな登録点の即時補完情報となるように、前記次の順次集約木のリーフに割り当てることを特徴とする請求項8乃至13のいずれか1項に記載のイベント順序証明方法。

[15] 所定のデジタル情報を生成するイベントの時系列において、あるイベントを生成した相対的な時刻、即ち時間的順序、を証明する証明要求を行う少なくとも1つの利用者装置と、利用者装置からの証明要求に対する証明書を作成する証明装置と、前記証明書の真偽を監査する監査装置とが通信ネットワークを介して相互に接続されたイベント順序証明システムにおけるイベント順序証明監査方法であって、

前記証明装置が前記利用者装置から第1の証明要求を受信する順序証明要求受信ステップと、

前記証明装置が前記第1の証明要求に含まれるデジタル情報から予め定めた手順に従って順次割当データを作成する順次割当データ計算ステップと、

前記証明装置が、一連の順次割当データを時刻順に有向木のリーフに左から順次割り当てることによって一定時間間隔ごとに1つの集約木が生成される順次集約木において、同一の親を有する複数の子に割り当てられたそれぞれの割当値を連接した連接値に所定の衝突困難一方向関数を適用した結果値を前記親の割当値とする計算方法により、計算可能なノードの割当値を計算するとともに、前記一定時間間隔終了後に前記順次集約木のルートに割り当てるルート値を計算する順序証明要求集

約ステップと、

前記証明装置が、前記順次割当データ、並びに前記順次割当データが割り当てられた順次集約木及び該順次集約木のリーフを特定する第1の順次集約木特定情報を含む第1の証明書を作成する証明書作成ステップと、

前記証明装置が前記第1の証明書を前記利用者装置に送信する証明書送信ステップと、

前記第1の証明要求が割り当てられた前記順次集約木のリーフを登録点として定義し、該登録点から前記順次集約木のルート値を計算するのに必要なノードに関する情報を前記第1の証明書の補完情報と定義し、該補完情報のうち、前記第1の証明要求を前記順次集約木に割り当てた時点において取得可能な補完情報を即時補完情報と定義すると、

前記証明装置が、複数の監査要求を前記順次集約木に割り当て、前記第1の証明書と同一の作成方法により、複数の監査用証明書を作成するとともに、各監査要求を前記順次集約木に割り当てた時点における監査用の即時補完情報を前記順次集約木から取得し、各監査用証明書に含める監査用証明書作成ステップと、

前記証明装置が前記複数の監査用証明書を前記監査装置に送信する監査用証明書送信ステップと、

前記証明装置が、前記第1の証明書送信後に、前記利用者装置からの前記第1の証明書の補完情報の要求を受信する補完情報要求受信ステップと、

前記証明装置が、前記補完情報の要求が割り当てられた前記順次集約木及び前記順次集約木のリーフを特定する第2の順次集約木特定情報、及び前記補完情報の要求を割り当てた時点において取得可能な補完情報を前記順次集約木から取得し、遅延補完情報とする遅延補完情報作成ステップと、

前記証明装置が前記第1の証明書の前記遅延補完情報を前記利用者装置に送信する遅延補完情報送信ステップと、

前記監査装置が、前記証明装置から前記複数の監査用証明書を受信する監査用証明書受信ステップと、

前記監査装置が、前記利用者装置から前記第1の証明書及び前記第1の証明書

の前記遅延補完情報を含む前記第1の証明書に対する監査要求を受信する監査要求受信ステップと、

前記監査装置が、前記複数の監査用証明書の中から、前記第1の証明書に対する監査要求の第1及び第2の順次集約木特定情報に基づいて、前記第1の証明書より生成された時間的順序が後、かつ前記遅延補完情報より生成された時間的順序が前である監査用証明書を選択する第1の監査用証明書選択ステップと、

前記監査装置が、前記順次集約木の特定のノードに対して、前記第1の監査用証明書選択ステップで選択された監査用証明書に含まれる該ノードの割当値と、前記第1の証明書に対する監査要求から計算された該ノードの割当値が一致するか否かの検証に基づいて、前記第1の証明書の正当性を監査し、前記第1の証明書の証明要求の受付時刻と前記第1の監査用証明書選択ステップで選択された監査用証明書の監査要求の受付時刻との前後関係を証明する第1の証明書監査ステップと、

前記監査装置が前記第1の証明書の監査結果を前記利用者装置に送信する監査結果送信ステップと、

を有することを特徴とするイベント順序証明監査方法。

[16] 前記監査用証明書受信ステップは、さらに、前記監査装置が前記第1の監査用証明書選択ステップで選択された監査用証明書を受信した第1の時刻を時刻提供装置から取得するステップを備え、

前記第1の証明書監査ステップにおいて、前記監査装置は、前記第1の証明書の前記証明要求の前記受付時刻が前記第1の時刻よりも時間的に前であることを示す区間時刻証を前記監査結果に含めることを特徴とする請求項15記載のイベント順序証明監査方法。

[17] 前記証明装置が、前記一定時間間隔終了後に前記監査用証明書作成ステップにおいて作成された前記複数の監査用証明書の前記補完情報すべてを前記順次集約木から取得し、各監査用証明書の遅延補完情報とする監査用遅延補完情報作成ステップと、

前記証明装置が前記複数の監査用証明書の前記遅延補完情報を前記監査装置に送信する監査用遅延補完情報送信ステップと、

前記監査装置が、前記複数の監査用証明書の中から、前記第1の証明書に対する監査要求の第1の順次集約木特定情報に基づいて、前記第1の証明書より時間的順序が前の監査用証明書を選択する第2の監査用証明書選択ステップと、

前記監査装置が、前記順次集約木の特定のノードに対して、前記第1の証明書に対する監査要求に含まれる該ノードの割当値と、前記第2の監査用証明書選択ステップで選択された監査用証明書及び該監査用証明書の前記遅延補完情報から計算された該ノードの割当値が一致するか否かの検証に基づいて、前記第1の証明書の正当性を監査し、前記第1の証明書の前記証明要求の前記受付時刻と前記第2の監査用証明書選択ステップで選択された監査用証明書の監査要求の受付時刻との前後関係を証明する第2の証明書監査ステップと、

をさらに有することを特徴とする請求項15又は16記載のイベント順序証明監査方法。

[18] 前記利用者装置又は他の利用者装置から第2の証明要求が為されたときには、前記監査装置が、前記第2の証明要求に対して作成された第2の証明書に対する監査結果と、前記第1及び第2の証明書の第1の順次集約木特定情報に基づいて、前記第1及び第2の証明書間における証明要求の受付時刻の前後関係を判定する証明書間順序判定ステップをさらに有し、

前記監査結果送信ステップにおいて、前記監査装置は、前記複数の証明書間における要求受付の時間的順序を前記監査結果に含めることを特徴とする請求項17記載のイベント順序証明監査方法。

[19] 前記監査装置が前記複数の監査用証明書及び前記複数の監査用証明書の遅延補完情報から前記順次集約木のルート値を計算するルート値計算ステップと、

前記監査装置が電子的に公表された前記順次集約木のルート値と前記計算されたルート値が一致するか否かの検証を行うルート値検証ステップと、

をさらに有することを特徴とする請求項17又は18記載のイベント順序証明監査方法。

[20] 前記監査装置が、前記第1の監査用証明書選択ステップで選択された監査用証明書及び該監査用証明書の遅延補完情報を前記利用者装置に送信する監査用補完

情報送信ステップをさらに有することを特徴とする請求項17乃至19のいずれか1項に記載のイベント順序証明監査方法。

[21] 前記監査用証明書受信ステップは、さらに、前記監査装置が前記第2の監査用証明書選択ステップで選択された監査要求を前記証明装置に送信した第2の時刻を時刻提供装置から取得するステップを有し、

前記第2の証明書監査ステップにおいて、前記監査装置は、前記第1の証明書の前記証明要求の前記受付時刻が前記第2の時刻より時間的に後であることを示す区間時刻証を監査結果に含めることを特徴とする請求項17乃至20のいずれか1項に記載のイベント順序証明監査方法。

[22] 前記第1の証明監査ステップにおいて、前記監査装置は、前記監査結果にデジタル署名を施すことを特徴とする請求項15乃至21のいずれか1項に記載のイベント順序証明監査方法。

[23] 所定のデジタル情報を生成するイベントの時系列において、あるイベントを生成した相対的な時刻、即ち時間的順序、を証明する証明要求を行い、証明書の作成を促す利用者装置と、該証明書の真偽を監査する監査装置とに通信ネットワークを介して相互に接続され、前記証明書を作成するイベント順序証明装置であって、

前記利用者装置から証明要求を受信する順序証明要求受信手段と、

前記証明要求に含まれるデジタル情報から予め定めた手順に従って順次割当データを作成する順次割当データ計算手段と、

一連の順次割当データを時刻順に有向木のリーフに左から順次割り当てることによって一定時間間隔ごとに1つの集約木が生成される順次集約木において、同一の親を有する複数の子に割り当てられたそれぞれの割当値を連接した連接値に所定の衝突困難一方向関数を適用した結果値を前記親の割当値とする計算方法により、計算可能なノードの割当値を計算するとともに、前記一定時間間隔終了後に前記順次集約木のルートに割り当てるルート値を計算する順序証明要求集約手段と、

前記順次割当データ、並びに前記順次割当データが割り当てられた順次集約木及び該順次集約木のリーフを特定する第1の順次集約木特定情報を含む証明書を作成する証明書作成手段と、

前記証明書を前記利用者装置に送信する証明書送信手段と、

前記証明要求が割り当てられた前記順次集約木のリーフを登録点と定義し、該登録点から前記順次集約木のルート値を計算するのに必要なノードに関する情報を前記証明書の補完情報と定義し、該補完情報のうち、前記証明要求を前記順次集約木に割り当てた時点において取得可能な補完情報を即時補完情報と定義すると、

前記証明要求を前記順次集約木に割り当てた以後に、第1の監査要求を前記順次集約木に割り当て、前記証明書と同一の作成方法により、第1の監査用証明書を作成するとともに、前記第1の監査要求を前記順次集約木に割り当てた時点における第1の監査用の即時補完情報を前記順次集約木から取得し、該第1の監査用証明書に含める監査用証明書作成手段と、

前記第1の監査用証明書を前記監査装置に送信する監査用証明書送信手段と、

前記第1の監査要求を前記順次集約木に割り当てた以後に、前記利用者装置からの前記証明書の補完情報の要求を受信する補完情報要求受信手段と、

前記補完情報の要求が割り当てられた前記順次集約木及び前記順次集約木のリーフを特定する第2の順次集約木特定情報、及び前記補完情報の要求を割り当てた時点において取得可能な補完情報を前記順次集約木から取得し、遅延補完情報とする遅延補完情報作成手段と、

前記証明書の前記遅延補完情報を前記利用者装置に送信する遅延補完情報送信手段と、

を有することを特徴とするイベント順序証明装置。

[24] 前記証明書作成手段は、前記第1の順次集約木特定情報に前記第1の証明書の即時補完情報を含めることを特徴とする請求項23記載のイベント順序証明装置。

[25] 前記監査用証明書作成手段は、さらに、前記証明要求を前記順次集約木に割り当てた以前に、第2の監査要求を前記順次集約木に割り当て、前記証明書と同一の作成方法により、第2の監査用証明書を作成するとともに、前記第2の監査要求を前記順次集約木に割り当てた時点における第2の監査用の即時補完情報を前記順次集約木から取得し、該第2の監査用証明書に含める手段を備え、

前記一定時間間隔終了後に前記監査用証明書作成手段で作成された前記第1及

び第2の監査用証明書の補完情報すべてを前記順次集約木から取得し、各監査用証明書の遅延補完情報とする監査用遅延補完情報作成手段と、

前記第1及び第2の監査用証明書の前記遅延補完情報を前記監査装置に送信する監査用遅延補完情報送信手段と、

をさらに有することを特徴とする請求項23又は24記載のイベント順序証明装置。

[26] 前記順次割当データ計算手段は、前記証明要求に含まれる前記デジタル情報に対して所定の衝突困難一方向関数を適用した結果値を前記順次割当データとして計算することを特徴とする請求項23乃至25のいずれか1項に記載のイベント順序証明装置。

[27] 前記証明書作成手段は、前記証明書にデジタル署名を施すことを特徴とする請求項23乃至26のいずれか1項に記載のイベント順序証明装置。

[28] 前記一定時間間隔終了後に前記順次集約木の前記ルート値を電子的に公表する電子的情報公表手段をさらに有することを特徴とする請求項23乃至27のいずれか1項に記載のイベント順序証明装置。

[29] 前記利用者装置から複数の証明要求が為されたときに、各証明要求を前記順次集約木に割り当てた時間的順序で、各証明要求に対する証明書を送信する手段を有することを特徴とする請求項23乃至28のいずれか1項に記載のイベント順序証明装置。

[30] 前記利用者装置から複数の証明要求が為されたときに、

前記順序証明要求集約手段により生成される前記順次集約木に関する情報を記憶する順次集約木記憶手段と、

前記順次集約木において、リーフa1より右に位置するリーフa2の割当処理が終了した時点で定まる前記リーフa1の遅延補完情報を、前記リーフa1の前記リーフa2における遅延補完情報といい、さらに、最新の証明要求から作成された順次割当データが割り当てられた前記順次集約木のリーフを新登録点とすると、

前記複数の証明要求の登録点に関する情報を記憶する登録点記憶手段と、

を有し、

前記証明書作成手段は、各記憶手段によって記憶された情報から、該新登録点の

順次割当データと、該順次割当データが割り当てられた前記順次集約木及び該順次集約木のリーフを特定する第1の順次集約木特定情報と、前記新登録点の即時補完情報と、前記利用者装置の過去のすべての登録点の前記新登録点における遅延補完情報と、を併せることによって前記新登録点に対する証明書を作成することを特徴とする請求項24記載のイベント順序証明装置。

[31] 前記利用者装置から複数の証明要求が為されたときに、

前記順序証明要求集約手段で生成される前記順次集約木に関する情報を記憶部に記憶する順次集約木記憶手段と、

前記順次集約木において、リーフa1より右に位置するリーフa2の割当処理が終了した時点で定まる前記リーフa1の遅延補完情報を、前記リーフa1の前記リーフa2における遅延補完情報といい、さらに、最新の証明要求から作成された順次割当データが割り当てられた前記順次集約木のリーフを新登録点とすると、

前記直前の登録点に関する情報を前記記憶部に記憶する登録点記憶手段と、

をさらに有し、

前記証明書作成手段は、各記憶手段によって記憶された情報から、該新登録点の順次割当データと、該順次割当データが割り当てられた前記順次集約木及び該順次集約木のリーフを特定する順次集約木特定情報と、該新登録点の即時補完情報を備える前記証明書と、前記利用者装置の前記直前の登録点の前記新登録点における遅延補完情報と、を併せることによって前記新登録点に対する証明書を作成することを特徴とする請求項24記載のイベント順序証明装置。

[32] 前記順次集約木記憶手段は、前記順次集約木に関する情報として、前記順次集約木において割当処理がされた各ノードの位置及び割当値を記憶することを特徴とする請求項30又は31記載のイベント順序証明装置。

[33] 前記順次集約木記憶手段は、前記新登録点の前記即時補完情報を記憶する第1のスタックと、前記利用者装置の前記直前の登録点の前記新登録点における前記遅延補完情報を記憶する第2のスタックとを有することを特徴とする請求項31記載のイベント順序証明装置。

[34] 前記一定時間間隔終了後に前記順次集約木の前記ルート値を電子的に公表する

電子的情報公表手段をさらに有することを特徴とする請求項30乃至33のいずれか1項に記載のイベント順序証明装置。

[35] 前記利用者装置は、前記一定時間間隔終了前に、前記イベント順序証明装置が運用を中断、あるいは前記順次集約木のルート値を計算するのに必要なデータを消失したときに、イベント順序証明装置の運用中断あるいはデータ消失の時点までに受信し記憶した証明書から、計算可能な割当値を持つ前記順次集約木のノードのうちで、その親のノードの割当値が計算できないような1つあるいは複数のノードの位置情報と割当値を、電子的に公表する利用者サイド電子的情報公表手段をさらに有することを特徴とする請求項30乃至34のいずれか1項に記載のイベント順序証明装置。

[36] 前記順序証明要求集約手段は、前記一定時間間隔終了後に前記順次集約木の前記ルート値を、次の順次集約木のリーフに割り当てられた新たな登録点の即時補完情報となるように、前記次の順次集約木のリーフに割り当てることを特徴とする請求項30乃至35のいずれか1項に記載のイベント順序証明装置。

[37] 所定のデジタル情報を生成するイベントの時系列において、あるイベントを生成した相対的な時刻、即ち時間的順序、を証明する証明要求を行う少なくとも1つの利用者装置と、利用者装置からの証明要求に対する証明書を作成する証明装置とに通信ネットワークを介して接続され、前記証明書の真偽を監査するイベント順序証明監査装置であって、

前記証明装置は、

前記利用者装置からの第1の証明要求を受信する順序証明要求受信手段と、

前記第1の証明要求に含まれるデジタル情報から予め定めた手順に従って順次割当データを作成する順次割当データ計算手段と、

一連の順次割当データを時刻順に有向木のリーフに左から順次割り当てることによって一定時間間隔ごとに1つの集約木が生成される順次集約木において、同一の親を有する複数の子に割り当てられたそれぞれの割当値を連接した連接値に所定の衝突困難一方向関数を適用した結果値を前記親の割当値とする計算方法により、計算可能なノードの割当値を計算するとともに、前記一定時間間隔終了後に前記順次

JP2005015085 / 2006-019143

2/3

Date: Feb 23, 2006

Recipient: IB

集約木のルートに割り当てるルート値を計算する順序証明要求集約手段と、

前記順次割当データ、並びに前記順次割当データが割り当てられた順次集約木及び該順次集約木のリーフを特定する第1の順次集約木特定情報を含む第1の証明書を作成する証明書作成手段と、

前記第1の証明書を前記利用者装置に送信する証明書送信手段と、

前記第1の証明要求が割り当てられた前記順次集約木のリーフを登録点と定義し、該登録点から前記順次集約木のルート値を計算するのに必要なノードに関する情報を前記第1の証明書の補完情報と定義し、該補完情報のうち、前記第1の証明要求を前記順次集約木に割り当てた時点において取得可能な補完情報を即時補完情報と定義すると、

複数の監査要求を前記順次集約木に割り当て、前記第1の証明書と同一の作成方法により、複数の監査用証明書を作成するとともに、前記複数の監査要求を前記順次集約木に割り当てた時点における監査用の前記即時補完情報を前記順次集約木から取得し、各監査用証明書に含める監査用証明書作成手段と、

前記複数の監査用証明書を前記監査装置に送信する監査用証明書送信手段と、

前記第1の証明書送信後に、前記利用者装置からの前記第1の証明書の補完情報の要求を受信する補完情報要求受信手段と、

前記補完情報の要求が割り当てられた前記順次集約木及び前記順次集約木のリーフを特定する第2の順次集約木特定情報、及び前記補完情報の要求を割り当てた時点において取得可能な補完情報を前記順次集約木から取得し、遅延補完情報とする遅延補完情報作成手段と、

前記第1の証明書の前記遅延補完情報を前記利用者装置に送信する遅延補完情報送信手段と、

を備え、

前記証明装置から前記複数の監査用証明書を受信する監査用証明書受信手段と、

前記利用者装置から前記第1の証明書及び前記遅延補完情報を含む前記第1の証明書に対する監査要求を受信する監査要求受信手段と、

前記複数の監査用証明書の中から、前記第1の証明書に対する監査要求の第1及び第2の順次集約木特定情報に基づいて、前記第1の証明書より生成された時間的順序が後、かつ前記遅延補完情報より生成された時間的順序が前である監査用証明書を選択する第1の監査用証明書選択手段と、

前記順次集約木の特定のノードに対して、前記第1の監査用証明書選択手段で選択された監査用証明書に含まれる該ノードの割当値と、前記第1の証明書に対する監査要求から計算された該ノードの割当値が一致するか否かの検証に基づいて、前記第1の証明書の正当性を監査し、前記第1の証明書の証明要求の受付時刻と前記第1の監査用証明書選択手段によって選択された監査用証明書の監査要求の受付時刻との前後関係を証明する第1の証明書監査手段と、

前記第1の証明書の監査結果を前記利用者装置に送信する監査結果送信手段と、

を備えることを特徴とするイベント順序証明監査装置。

[38] 前記監査用証明書受信手段は、さらに、前記第1の監査用証明書選択手段によって選択された監査用証明書を受信した第1の時刻を時刻提供装置から取得する手段を備え、

前記第1の証明書監査手段は、前記第1の証明書の前記証明要求の前記受付時刻が前記第1の時刻よりも時間的に前であることを示す区間時刻証を前記監査結果に含めることを特徴とする請求項37記載のイベント順序証明監査装置。

[39] 前記証明装置は、

前記一定時間間隔終了後に前記監査用証明書作成手段で作成された前記複数の監査用証明書の補完情報すべてを前記順次集約木から取得し、各監査用証明書の遅延補完情報とする監査用遅延補完情報作成手段と、

前記複数の監査用証明書の前記遅延補完情報を前記監査装置に送信する監査用遅延補完情報送信手段と、

をさらに備え、

前記複数の監査用証明書の中から、前記第1の証明書に対する監査要求の第1の順次集約木特定情報に基づいて、前記第1の証明書より時間的順序が前の監査用

証明書を選択する第2の監査用証明書選択手段と、

前記順次集約木の特定のノードに対して、前記第1の証明書に対する監査要求に含まれる該ノードの割当値と、前記第2の監査用証明書選択手段で選択された監査用証明書及び該監査用証明書の前記遅延補完情報から計算された該ノードの割当値が一致するか否かの検証に基づいて、前記第1の証明書の正当性を監査し、前記第1の証明書の前記証明要求の前記受付時刻と前記第2の監査用証明書選択手段によって選択された監査用証明書の監査要求の受付時刻の前後関係を証明する第2の証明書監査手段と、

をさらに備えることを特徴とする請求項37又は38記載のイベント順序証明監査装置。

[40] 前記利用者装置又は他の利用者装置から第2の証明要求が為されたときに、前記第2の証明要求に対して作成された第2の証明書に対する監査結果と、前記第1及び第2の証明書の第1の順次集約木特定情報に基づいて、前記第1及び第2の証明書間における証明要求の受付時刻の前後関係を判定する証明書間順序判定手段をさらに備え、

前記監査結果送信手段は、前記複数の証明書間における要求受付の時間的順序を前記監査結果に含めることを特徴とする請求項39記載のイベント順序証明監査装置。

[41] 前記複数の監査用証明書及び該複数の監査用証明書の遅延補完情報から前記順次集約木のルート値を計算するルート値計算手段と、

電子的に公表された前記順次集約木のルート値と前記計算されたルート値が一致するか否かの検証を行うルート値検証手段と、

をさらに備えることを特徴とする請求項39又は40記載のイベント順序証明監査装置。

[42] 前記第1の監査用証明書選択手段で選択された監査用証明書及び該監査用証明書の遅延補完情報を前記利用者装置に送信する監査用補完情報送信手段をさらに備えることを特徴とする請求項39乃至41のいずれか1項に記載のイベント順序証明監査装置。

[43] 前記監査用証明書受信手段は、さらに、前記第2の監査用証明書選択手段によって選択された監査要求を前記証明装置に送信した第2の時刻を時刻提供装置から取得する手段を備え、

前記第2の証明書監査手段は、前記第1の証明書の前記証明要求の前記受付時間が前記第2の時刻より時間的に後であることを示す区間時刻証を監査結果に含めることを特徴とする請求項39乃至42のいずれか1項に記載のイベント順序証明監査装置。

[44] 前記第1の証明書監査手段は、前記監査結果にデジタル署名を施すことを特徴とする請求項39乃至43のいずれか1項に記載のイベント順序証明監査装置。

[45] 請求項1乃至14のいずれか1項に記載のイベント順序証明方法の各ステップを前記証明装置に実行させることを特徴とするイベント順序証明プログラム。

[46] 請求項15乃至22のいずれか1項に記載のイベント順序証明監査方法の各ステップを前記監査装置に実行させることを特徴とするイベント順序証明監査プログラム。

[47] 所定のデジタル情報を生成するイベントの時系列において、あるイベントを生成した相対的な時刻、即ち時間的順序、を証明する証明要求を行う少なくとも1つの利用者装置と、利用者装置からの証明要求に対する証明書を作成する証明装置と、前記証明書の真偽を監査する監査装置とが通信ネットワークを介して相互に接続されたイベント順序証明検証システムにおける前記利用者装置のためのイベント順序証明検証プログラムであって、

前記証明装置は、

前記利用者装置からの第1の証明要求を受信する順序証明要求受信手段と、

前記第1の証明要求に含まれるデジタル情報から予め定めた手順に従って順次割当データを作成する順次割当データ計算手段と、

一連の順次割当データを時刻順に有向木のリーフに左から順次割り当てることによって一定時間間隔ごとに1つの集約木が生成される順次集約木において、同一の親を有する複数の子に割り当てられたそれぞれの割当値を連接した連接値に所定の衝突困難一方向関数を適用した結果値を前記親の割当値とする計算方法により、計算可能なノードの割当値を計算するとともに、前記一定時間間隔終了後に前記順次

集約木のルートに割り当てるルート値を計算する順序証明要求集約手段と、

前記順次割当データ、並びに前記順次割当データが割り当てられた順次集約木及び該順次集約木のリーフを特定する第1の順次集約木特定情報を含む第1の証明書を作成する証明書作成手段と、

前記第1の証明書を前記利用者装置に送信する証明書送信手段と、

前記第1の証明要求が割り当てられた前記順次集約木のリーフを登録点と定義し、該登録点から前記順次集約木のルート値を計算するのに必要なノードに関する情報を前記第1の証明書の補完情報と定義し、該補完情報のうち、前記第1の証明要求を前記順次集約木に割り当てた時点において取得可能な補完情報を即時補完情報と定義すると、

複数の監査要求を前記順次集約木に割り当て、前記第1の証明書と同一の作成方法により、複数の監査用証明書を作成するとともに、前記複数の監査要求を前記順次集約木に割り当てた時点におけるそれぞれの監査用の即時補完情報を前記順次集約木から取得し、前記複数の監査用証明書に含める監査用証明書作成手段と、

前記複数の監査用証明書を前記監査装置に送信する監査用証明書送信手段と、

前記第1の証明書送信後に、前記利用者装置からの前記第1の証明書の補完情報の要求を受信する補完情報要求受信手段と、

前記補完情報の要求が割り当てられた前記順次集約木及び前記順次集約木のリーフを特定する第2の順次集約木特定情報、及び前記補完情報の要求を割り当てた時点において取得可能な補完情報を前記順次集約木から取得し、遅延補完情報とする遅延補完情報作成手段と、

前記第1の証明書の前記遅延補完情報を前記利用者装置に送信する遅延補完情報送信手段と、

を有し、

前記監査装置は、

前記証明装置から、前記複数の監査用証明書を受信する監査用証明書受信手段と、

前記利用者装置から、前記第1の証明書及び前記遅延補完情報を含む前記第1

の証明書に対する監査要求を受信する監査要求受信手段と、

前記複数の監査用証明書の中から、前記第1の証明書に対する監査要求の第1及び第2の順次集約木特定情報に基づいて、前記第1の証明書より生成された時間的順序が後、かつ前記遅延補完情報より生成された時間的順序が前である監査用証明書を選択する第1の監査用証明書選択手段と、

前記順次集約木の特定のノードに対して、前記第1の監査用証明書選択手段によって選択された監査用証明書に含まれる該ノードの割当値と、前記第1の証明書に対する監査要求から計算された該ノードの割当値が一致するか否かの検証に基づいて、前記第1の証明書の正当性を監査し、前記第1の証明書の証明要求の受付時刻と前記第1の監査用証明書選択手段によって選択された監査用証明書の監査要求の受付時刻の前後関係を証明する第1の証明書監査手段と、

前記第1の証明書の監査結果を前記利用者装置に送信する監査結果送信手段と

、

を有し、

前記第1の証明要求を前記証明装置に送信する順序証明要求送信ステップと、

前記証明装置から、前記第1の証明書を受信する証明書受信ステップと、

前記第1の証明書の前記補完情報の要求を前記証明装置に送信する補完情報要求送信ステップと、

前記証明装置から、前記第1の証明書の前記補完情報を受信する補完情報受信ステップと、

前記監査要求を前記監査装置に送信する監査要求送信ステップと、

前記第1の証明書の監査結果を受信する監査結果受信ステップと、

を前記利用者装置に実行させることを特徴とするイベント順序証明検証プログラム。

[48] 前記監査用証明書受信手段は、前記第1の監査用証明書選択手段によって選択された監査用証明書を受信した第1の時刻を時刻提供装置から取得する手段を有し

、

前記第1の証明書監査手段は、前記第1の証明書の前記証明要求の前記受付時刻が前記第1の時刻よりも時間的に前であることを示す区間時刻証を前記監査結果

に含め、

前記第1の証明要求を前記証明装置に送信する時点の第3の時刻を前記時刻提供装置から取得し、該第3の時刻を所定の手順に従って計算した値を前記第1の証明要求に含める順序証明要求作成ステップを

前記利用者装置に実行させることを特徴とする請求項47記載のイベント順序証明検証プログラム。

[49] 前記証明装置は、

前記一定時間間隔終了後に前記監査用証明書作成手段で作成された前記複数の監査用証明書の補完情報すべてを前記順次集約木から取得し、各監査用証明書の遅延補完情報とする監査用遅延補完情報作成手段と、

前記複数の監査用証明書の前記遅延補完情報を前記監査装置に送信する監査用遅延補完情報送信手段と、

を有し、

前記監査装置は、

前記複数の監査用証明書の中から、前記第1の証明書に対する監査要求の第1の順次集約木特定情報に基づいて、前記第1の証明書より時間的順序が前の監査用証明書を選択する第2の監査用証明書選択手段と、

前記順次集約木の特定のノードに対して、前記第1の証明書に対する監査要求に含まれる該ノードの割当値と、前記第2の監査用証明書選択手段で選択された監査用証明書及び該監査用証明書の遅延補完情報から計算された該ノードの割当値が一致するか否かの検証に基づいて、前記第1の証明書の正当性を監査し、前記第1の証明書の前記証明要求の前記受付時刻と前記第2の監査用証明書選択手段によって選択された監査用証明書の監査要求の受付時刻の前後関係を証明する第2の証明書監査手段と、

を有することを特徴とする請求項47又は48記載のイベント順序証明検証プログラム。

[50] 前記監査装置は、

前記利用者装置又は他の利用者装置から第2の証明要求が為されたときに、前記

第2の証明要求に対して作成された第2の証明書に対する監査結果と、前記第1及び第2の証明書の第1の順次集約木特定情報に基づいて、前記第1及び第2の証明書間における証明要求の受付時刻の前後関係を判定する証明書間順序判定手段を有し、

前記監査結果送信手段は、前記第1及び第2の証明書間における前記証明要求の前記受付時間の前記前後関係を前記監査結果に含め、

前記第1の証明書に対する監査要求は、前記第2の証明書との時間的順序の判定要求を含むことを特徴とする請求項49記載のイベント順序証明検証プログラム。

[51] 前記監査装置は、

前記第1の監査用証明書選択手段で選択された監査用証明書及び該監査用証明書の遅延補完情報を前記利用者装置に送信する監査用補完情報送信手段を有し、

前記監査装置から送信された監査用証明書及び該監査用証明書の遅延補完情報を受信するステップを

前記利用者装置に実行させることを特徴とする請求項49記載のイベント順序証明検証プログラム。

[52] 前記監査用証明書受信手段は、前記第2の監査用証明書選択手段によって選択された監査要求を前記証明装置に送信した第2の時刻を時刻提供装置から取得する手段を有し、

第2の証明書監査手段は、前記第1の証明書の前記証明要求の前記受付時刻が前記第2の時刻より時間的に後であることを示す区間時刻証を監査結果に含め、

前記第1の証明要求を前記証明装置に送信した時点の第3の時刻を前記時刻提供装置から取得し、該第3の時刻を所定の手順に従って計算した値を前記第1の証明要求に含める順序証明要求作成ステップを

前記利用者装置に実行させることを特徴とする請求項48乃至51のいずれか1項に記載のイベント順序証明検証プログラム。

[53] 前記証明装置から受信した前記第1の証明書、及び前記一定時間間隔終了後に取得した該第1の証明書の補完情報すべてから、前記順次集約木のルート値を計算するルート値計算ステップと、

前記一定時間間隔終了後に電子的に公表された前記順次集約木のルート値と前記計算されたルート値が一致するか否かの検証を行うルート値検証ステップと、

を

前記利用者装置に実行させることを特徴とする請求項47乃至52のいずれか1項に記載のイベント順序証明検証プログラム。

[54] 所定のデジタル情報を生成するイベントの時系列において、あるイベントを生成した相対的な時刻、即ち時間的順序、を証明する証明要求を行う第1及び第2の利用者装置と、各利用者装置からの複数の証明要求に対して複数の証明書を作成するイベント順序証明装置とに通信ネットワークを介して相互に接続されたコンピュータに証明書の正当性を検証させるイベント順序証明検証プログラムであって、

前記イベント順序証明装置は、

前記第1及び第2の利用者装置から複数の証明要求を受信する順序証明要求受信手段と、

各証明要求に含まれるデジタル情報から予め定めた手順に従って順次割当データを作成する順次割当データ計算手段と、

一連の順次割当データを時刻順に有向木のリーフに左から順次割り当て、一定時間間隔ごとに1つの集約木が生成される順次集約木において、同一の親を有する複数の子に割り当てられたそれぞれの割当値を連接した連接値に所定の衝突困難一方向関数を適用した結果値を前記親の割当値とする計算方法により、計算可能なノードの割当値を計算するとともに、前記一定時間間隔終了後に前記順次集約木のルートに割り当てるルート値を計算する順序証明要求集約手段と、

前記順序証明要求集約手段で生成される順次集約木に関する情報を記憶する順次集約木記憶手段と、

各証明要求から作成された順次割当データが割り当てられた前記順次集約木のリーフを登録点と定義し、該登録点から前記順次集約木のルート値を計算するのに必要なノードに関する情報を前記登録点の補完情報と定義し、該補完情報のうち、前記順次割当データを前記順次集約木に割り当てた時点において取得可能な補完情報を即時補完情報、前記順次割当データを前記順次集約木に割り当てた時点以後

において取得可能な補完情報を遅延補完情報と定義し、リーフa1より右に位置するリーフa2の割当処理が終了した時点で定まる前記リーフa1の遅延補完情報を、前記リーフa1の前記リーフa2における遅延補完情報といい、さらに、最新の前記要求から作成された順次割当データが割り当てられた前記順次集約木のリーフを新登録点とすると、

利用者装置ごとに前記複数の証明要求の登録点に関する情報を記憶する登録点記憶手段と、

各記憶手段によって記憶された情報から、該新登録点の順次割当データと、該順次割当データが割り当てられた前記順次集約木及び該順次集約木のリーフを特定する順次集約木特定情報と、前記新登録点の即時補完情報と、各利用者装置の過去のすべての登録点の新登録点における遅延補完情報と、を併せることによって前記新登録点に対する証明書を作成する証明書作成手段と、

前記作成された複数の証明書を前記利用者装置に送信する証明書送信手段と、

を有し、

各利用者装置は、

複数の証明要求を前記イベント順序証明装置に送信する証明要求送信手段と、

前記イベント順序証明装置から前記複数の証明要求に対する前記複数の証明書を受信する証明書受信手段と、

前記受信した複数の証明書を記憶する証明書記憶手段と、

前記受信し記憶した複数の証明書のうち、検証対象の証明書を検証するコンピュータに送信する検証要求送信手段と、

前記コンピュータから前記検証対象の証明書に対する検証結果を受信する検証結果受信手段と、

を有し、

前記第1及び第2の利用者装置から検証対象の証明書を1つずつ受信するか、或いは前記第1の前記利用者装置から検証対象の証明書を2つ受信する証明書受信ステップと、

前記受信した2つの証明書の順次集約木特定情報に基づいて、前記2つの証明書

のうち発行された順序が時間的に前であると判断された証明書を第1の証明書、後であると判断された証明書を第2の証明書とすると、前記第1の証明書を送信した利用者装置に対して前記第2の証明書の順次集約木特定情報を送信する順次集約木特定情報送信ステップと、

前記第1の証明書を送信した利用者装置から、前記第1の証明書の前記第2の証明書の発行以降の登録点における遅延補完情報を受信する遅延補完情報受信ステップと、

前記順次集約木の特定のノードに対して、前記第2の証明書に含まれるノードの割当値と、前記第1の証明書および前記遅延補完情報から計算されたノードの割当値が一致するか否かの検証に基づいて、各証明書の正当性及び前記第1の証明書の登録点が前記第2の証明書の登録点より時間的に前であることを証明する検証ステップと、

検証結果を前記第1及び第2の利用者装置、或いは前記第1又は第2の利用者装置に送信する検証結果送信ステップと、

を前記コンピュータに実行させることを特徴とするイベント順序証明検証プログラム。

[55] 各利用者装置は、

前記一定時間間隔終了前に、前記イベント順序証明装置が運用を中断、あるいは前記順次集約木のルート値を計算するのに必要なデータを消失したとき、イベント順序証明装置の運用中断あるいはデータ消失の時点までに受信し記憶した証明書から、計算可能な割当値を持つ前記順次集約木のノードのうちで、その親のノードの割当値が計算できないような1つあるいは複数のノードの位置情報と割当値を、電子的に公表する利用者サイド電子的情報公表手段、

を有し、

前記一定時間間隔終了前に、前記イベント順序証明装置が運用を中断、あるいは前記順次集約木のルート値を計算するのに必要なデータを消失したとき、前記利用者装置により前記利用者サイド電子的情報公表手段で公表されたノードの割当値と、前記証明書受信ステップで受信したデータと前記遅延補完情報受信ステップで受

信したデータから該ノード割当値が計算できるときには計算されたノードの割当値が一致するか否かにより、前記証明書受信ステップで受信したデータと前記遅延補完情報受信ステップで受信したデータが改ざんされていないことの検証を行う利用者サイド公表値による検証ステップ

を前記コンピュータに実行させることを特徴とする請求項54記載のイベント順序証明検証プログラム。

[56] 所定のデジタル情報を生成するイベントの時系列において、あるイベントを生成した相対的な時刻、即ち時間的順序、を証明する証明要求を行う第1及び第2の利用者装置と、各利用者装置からの複数の証明要求に応えて複数の証明書を作成するイベント順序証明装置とに通信ネットワークを介して相互に接続されたコンピュータに証明書の正当性を検証させるイベント順序証明検証プログラムであって、

前記イベント順序証明装置は、

前記第1及び第2の利用者装置から複数の証明要求を受信する順序証明要求受信手段と、

各証明要求に含まれるデジタル情報から予め定めた手順に従って順次割当データを作成する順次割当データ計算手段と、

一連の順次割当データを時刻順に有向木のリーフに左から順次割り当て、一定時間間隔ごとに1つの集約木が生成される順次集約木において、同一の親を有する複数の子に割り当てられたそれぞれの割当値を連接した連接値に所定の衝突困難一方向関数を適用した結果値を前記親の割当値とする計算方法により、計算可能なノードの割当値を計算するとともに、前記一定時間間隔終了後に前記順次集約木のルートに割り当てるルート値を計算する順序証明要求集約手段と、

前記順序証明要求集約手段で生成される順次集約木に関する情報を記憶する順次集約木記憶手段と、

各証明要求から作成された順次割当データが割り当てられた前記順次集約木のリーフを登録点と定義し、該登録点から前記順次集約木のルート値を計算するのに必要な他のノードに関する情報を前記登録点の補完情報と定義し、該補完情報のうち、前記順次割当データを前記順次集約木に割り当てた時点において取得可能な補

完情報を即時補完情報、前記順次割当データを前記順次集約木に割り当てた時点以後において取得可能な補完情報を遅延補完情報と定義し、リーフa1より右に位置するリーフa2の割当処理が終了した時点で定まる前記リーフa1の遅延補完情報を、前記リーフa1の前記リーフa2における遅延補完情報といい、さらに、最新の前記要求から作成された順次割当データが割り当てられた前記順次集約木のリーフを新登録点とすると、

利用者装置ごとに前記直前の登録点に関する情報を記憶する登録点記憶手段と、

各記憶手段によって記憶された情報から、該新登録点の順次割当データと、該順次割当データが割り当てられた順次集約木及び該順次集約木のリーフを特定する順次集約木特定情報と、新登録点の即時補完情報と、前記利用者装置の前記直前の登録点の前記新登録点における遅延補完情報と、を併せることによって前記新登録点に対する証明書を作成する証明書作成手段と、

作成された証明応答を前記利用者装置に送信する証明応答送信手段と、

を有し、

各利用者装置の各登録点のうち、前記順次集約木の最も右に割り付けられた登録点を暫定終端点とし、該暫定終端点の割付処理が終了した時点において、所定の登録点の取得可能な補完情報すべてを計算することを、前記所定の登録点の証明書に対するインクリメンタル完全化と定義すると、

各利用者装置は、

複数の証明要求を前記イベント順序証明装置に送信する証明要求送信手段と、

前記イベント順序証明装置から前記複数の証明要求に対する前記複数の証明書を受信する証明書受信手段と、

前記受信した複数の証明書を記憶する証明書記憶手段と、

前記受信し記憶した複数の証明書のうち、検証対象の証明書に対して前記インクリメンタル完全化の処理を行うインクリメンタル完全化手段と、

前記インクリメンタル完全化された証明書を検証する検証要求をコンピュータに送信する検証要求送信手段と、

前記コンピュータから前記検証対象の前記証明書に対する検証結果を受信する検

証結果受信手段と、

を有し、

前記第1及び第2の利用者装置から検証対象の証明書を1つずつ受信するか、或いは前記第1の利用者装置から検証対象の証明書を2つ受信する証明書受信ステップと、

前記受信した2つの証明書の順次集約木特定情報に基づいて、前記2つの証明書のうち発行された順序が時間的に前であると判断された証明書を第1の証明書、後であると判断された証明書を第2の証明書とすると、前記第1の証明書を送信した利用者装置に、前記第2の証明書の順次集約木特定情報を送信する順次集約木特定情報送信ステップと、

前記第1の証明書を送信した利用者装置から、前記第1の証明書の前記第2の証明書の発行以降の登録点における遅延補完情報を受信する遅延補完情報受信ステップと、

前記順次集約木の特定のノードに対して、前記第2の証明書に含まれるノードの割当値と、前記第1の証明書および前記遅延補完情報から計算されたノードの割当値が一致するか否かの検証に基づいて、各証明書の正当性及び前記第1の証明書の登録点が前記第2の証明書の登録点より時間的に前であることを証明する検証ステップと、

検証結果を前記第1及び第2の利用者装置、或いは前記第1又は第2の利用者装置に送信する検証結果送信ステップと、

を前記コンピュータに実行させることを特徴とするイベント順序証明検証プログラム。

[57] 各利用者装置は、

前記一定時間間隔終了前に、前記イベント順序証明装置が運用を中断、あるいは前記順次集約木のルート値を計算するのに必要なデータを消失したとき、イベント順序証明装置の運用中断あるいはデータ消失の時点までに受信し記憶した証明書から、計算可能な割当値を持つ順次集約木のノードのうちで、その親のノードの割当値が計算できないような1つあるいは複数のノードの位置情報と割当値を、電子的に公

表する利用者サイド電子的情報公表手段、

を有し、

前記一定時間間隔終了前に、前記イベント順序証明装置が運用を中断、あるいは前記順次集約木のルート値を計算するのに必要なデータを消失したとき、前記利用者装置により前記利用者サイド電子的情報公表手段で公表されたノードの割当値と、前記証明書受信ステップで受信したデータと前記遅延補完情報受信ステップで受信したデータから該ノード割当値が計算できるときには計算されたノードの割当値が一致するか否かにより、前記証明書受信ステップで受信したデータと前記遅延補完情報受信ステップで受信したデータが改ざんされていないことの検証を行う利用者サイド公表値による検証ステップ

を前記コンピュータに実行させることを特徴とする請求項56記載のイベント順序証明検証プログラム。

[58] 前記利用者装置から複数の証明要求が為されたときに、

前記順序証明要求集約手段で生成される前記順次集約木に関する情報を記憶する順次集約木記憶手段と、

前記順次集約木において、リーフa1より右に位置するリーフa2の割当処理が終了した時点で定まる前記リーフa1の遅延補完情報を、前記リーフa1の前記リーフa2における遅延補完情報といい、さらに、最新の証明要求から作成された順次割当データが割り当てられた前記順次集約木のリーフを新登録点とすると、

前記直前の登録点に関する情報を記憶する登録点記憶手段と、

各記憶手段によって記憶された情報から、該新登録点の順次割当データと、該順次割当データが割り当てられた前記順次集約木及び該順次集約木のリーフを特定する順次集約木特定情報と、前記新登録点の即時補完情報を備える前記証明書と、前記利用者装置の前記直前の登録点の前記新登録点における遅延補完情報と、を併せることによって前記新登録点に対する証明書を作成する前記証明書作成手段と、

前記作成された複数の証明書を前記利用者装置に送信する証明書送信手段と、

を有し、

前記利用者装置の各登録点のうち、前記順次集約木の最も右に割り付けられた登録点を暫定終端点と定義し、該暫定終端点の割付処理が終了した時点において、所定の登録点の取得可能な補完情報すべてを計算することを、前記所定の登録点の証明書に対するインクリメンタル完全化と定義すると、

前記複数の証明要求を前記証明装置に送信する要求送信ステップと、

前記証明装置から前記複数の証明要求に対する前記複数の証明書を受信する証明書受信ステップと、

前記受信した複数の証明書を記憶する証明書記憶ステップと、

前記受信し記憶した複数の証明書のうち、検証対象の証明書に対して前記インクリメンタル完全化の処理を行うインクリメンタル完全化ステップと、

を前記利用者装置に実行させることを特徴とする請求項47に記載のイベント順序証明検証プログラム。

[59] 前記インクリメタル完全化は、前記利用者装置が前記証明装置から受信し記憶した前記複数の証明書を用いて、木構造を構成することなく実行されることを特徴とする請求項56乃至58のいずれか1項に記載のイベント順序証明検証プログラム。

[60] 前記インクリメタル完全化は、所定の登録点の、前記暫定終端点の割付処理が終了した時点において取得可能な補完情報の各要素に対して、前記利用者装置が前記証明装置から受信し記憶した1つあるいは複数の証明書の中から該要素を直接含むかあるいは該要素を計算するために十分な情報含むような1つの証明書を選出し、該証明書から該要素を計算することにより実行されることを特徴とする請求項59に記載のイベント順序証明検証プログラム。

[61] 前記インクリメンタル完全化は、前記利用者装置の前記暫定終端点より左に位置するすべての登録点に対して行うことを特徴とする請求項59記載のイベント順序証明検証プログラム。

[62] 前記暫定終端点の、左に位置する前記利用者装置の登録点a1とその左に位置し前記登録点a1に最も近い該利用者装置のもう一つの登録点a2について、

前記登録点a1の該暫定終端点の割付処理が終了した時点において取得可能な補完情報の全てと、前記登録点a2及びa1における受理証明書から、前記登録点a2の

該暫定終端点の割付処理が終了した時点において取得可能な補完情報の全てを計算することを完全化波及処理と定義すると、

前記インクリメタル完全化は、

前記暫定終端点の、左に位置し、該暫定終端点に最も近い、前記利用者装置の登録点aに対して該暫定終端点の割付処理が終了した時点において取得可能な補完情報すべてを前記利用者装置が受信し記憶した証明書から取得あるいは計算することから始まり、暫定終端点の左に位置する各登録点の該暫定終端点の割付処理が終了した時点において取得可能な補完情報すべてを計算する処理を、このような登録点のうち一番右に位置する前記登録点aからはじめ、前記完全化波及処理を用いて、順次その左に位置する登録点に対して実行することにより木構造を構成することなく実行されることを特徴とする請求項61に記載のイベント順序証明検証プログラム。

[63] 前記インクリメタル完全化は、前記暫定終端点までの各登録点を適宜抽出し、この抽出された登録点間の局所領域に分割し、分割された各局所領域において最も右に割り付けられた登録点を暫定終端点と仮定して、インクリメタル完全化を行うとともに、抽出された各登録点の取得可能な補完情報すべてを計算する方法により行われることを特徴とする請求項56乃至62のいずれか1項に記載のイベント順序証明検証プログラム。

[64] 前記証明装置は、

前記一定時間間隔終了後に前記順次集約木の前記ルート値を電子的に公表する電子的情報公表手段を有し、

前記一定時間間隔終了後に、前記所定の登録点に関する情報と前記インクリメンタル完全化ステップで計算された補完情報から、前記順次集約木のルート値を計算するルート値計算ステップと、

電子的に公表された前記順次集約木の前記ルート値と前記計算されたルート値が一致するか否かの検証を行うルート値検証ステップと、

を前記利用者装置に実行させることを特徴とする請求項56乃至63のいずれか1項に記載のイベント順序証明検証プログラム。

[65] 請求項48又は52記載のイベント順序証明検証プログラムを実行する利用者装置が前記要求に付した時刻を検証するコンピュータが読み取り可能なイベント時刻検証プログラムであって、

前記監査結果を取得する監査結果取得ステップと、

前記監査結果に対応する前記要求を取得する順序証明要求取得ステップと、

前記第3の時刻と、前記第1又は第2の時刻のうち少なくとも1以上との時間差に基づいて、前記第3の時刻の正当性を判定する時刻検証ステップと、

前記判定結果を出力するステップと、

を前記コンピュータに実行させることを特徴とするイベント時刻検証プログラム。